PROTOCOLOS DE ENRUTAMIENTO

JOSE FRANCISCO ANGULO JUAN

PEDRO LUIS CAMACHO JORGE

Director (a)
Margarita Upegui Ferrer
MSc. en Ciencias Computacionales

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

CARTAGENA DE INDIAS, DT Y C.

JUNIO DEL 2006

PROTOCOLOS DE ENRUTAMIENTO

JOSE FRANCISCO ANGULO JUAN

PEDRO LUIS CAMACHO JORGE

Trabajo final presentado como requisito parcial

Aprobar el Minor en Telecomunicaciones

Director (a)
Margarita Upegui Ferrer
MSc. en Ciencias Computacionales

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

MINOR EN TELECOMUNICACIONES

CARTAGENA DE INDIAS, DT Y C.
JUNIO DEL 2006

Cartagena de Indias Junio del 2006

Señores

Universidad Tecnológica de Bolívar

Comité de Evaluación de Proyectos

Ciudad

Estimados señores

Con el mayor respeto nos dirigimos a ustedes para poner a su disposición el trabajo final titulado **"PROTOCOLOS DE ENRUTAMIENTO"** el cual fue elaborado por los estudiantes **JOSE FRANCISCO ANGULO JUAN** y **PEDRO LUIS CAMACHO JORGE** para la evaluación del trabajo final del Minor en Telecomunicaciones.

Esperamos que este proyecto sea de su mayor agrado.

Cordialmente,

---------- ----------

José Francisco Angulo Juan Pedro Luís Camacho Jorge

Código: 0004061 Código: 0004097

TABLA DE CONTENIDO

Páginas

1. INTRODUCCION

Los protocolos de ruteo IP han evolucionado con el paso del tiempo. Estos se efectúan por medio del mantenimiento de una tabla de ruteo en cada dispositivo del medio y en cada sistema final. Estas tablas de ruteo pueden ser estáticas o dinámicas dependiendo de las condiciones que se presenten entre las conexiones de redes. Para utilizar todas las normas o protocolos que se mencionaran a continuación se debe tener en cuenta que los protocolos de ruteo en una conexión de redes funcionan de modo similar a los que se utilizan en redes de conmutación de paquetes, todo esto para intercambiar información sobre accesibilidad y retardos de tráfico.

En una conexión de redes, los dispositivos de ruteo son responsables de recibir y reenviar los paquetes a través del conjunto de redes interconectadas. Un protocolo común de ruteo, al que nos referimos como *Protocolo Interior de Ruteo* (IRP), distribuye información entre los dispositivos de ruteo dentro de un AS (sistema autónomo), a su vez el protocolo que se encarga para pasar información de ruteo entre diferentes AS se conoce como *Protocolo Exterior de Ruteo* (ERP).

Los protocolos Border Gateway Protocol (BGP) permiten la comunicación entre dominios distintos de AS. Así un AS es un grupo de ruteadores que

utiliza un mismo protocolo de ruteo. Cada AS puede ser dividido en un número de Áreas; un ruteador con múltiples interfaces puede participar de múltiples áreas. Estos ruteador se denominan ruteador de borde y mantienen separadas las bases de datos topológicas de cada área.

El protocolo BGP reemplaza al EGP en la Internet y trabaja sobre TCP. Permite el tráfico dentro de un AS entre ruteador pares (IBGP para Interior) o entre sistemas autónomos (EBGP para Exterior) y el pasaje por un sistema autónomo que no opera con BGP. Normalmente es usado entre operadores ISP. La versión IBGP es más flexible, entrega varias vías de conexión en el interior del AS y dispone de una vista del exterior gracias a EBGP. Cuando un ruteador se conecta a la red el BGP permite intercambiar las tablas de rutas completas. Para terminar analizaremos las diferentes estrategias que utilizan estos protocolos para redes interconectadas sabiendo que estas se basan en tres enfoques para recopilar y utilizar la información de ruteo por vector distancia, por estado de enlace y por vector camino.

2. FUNDAMENTACIÓN

2.1 DIRECCIONAMIENTO IP

2.1.2 TRES TIPOS DE DIRECCIONES IP

Cada anfitrión en una red de redes TCP/IP tiene asegurada una dirección de número entero de 32 bits que se utiliza en todas las comunicaciones con dicho anfitrión.

Los detalles de una dirección IP nos ayudan a entender mejor las ideas abstractas. En el caso más sencillo, cada anfitrión conectado a la red de redes tiene asignado un identificador universal de 32 bits como su dirección dentro de la red. Los bits de dirección IP de todos los anfitriones en una red comparten un prefijo común.

Conceptualmente, cada dirección es un par (*netid, hostid*), en donde *netid* identifica una red y *hostid* un anfitrión dentro de la red. En la práctica, cada dirección IP debe tener una de las primeras tres formas mostradas en la figura 1.[1]

Definida una dirección IP, se puede determinar su tipo según los tres bits de orden, de los que son necesarios sólo dos bits para distinguir entre los tres tipos primarios.

[1] La cuarta forma reservada para la multidifusión en la red de redes.

- Las direcciones tipo A, que se utilizan para pocas redes que tienen más de 2^{16} de anfitriones (por ejemplo, 65.536), asignan 7 bits al campo netid y 24 bits al hostid.
- Las direcciones tipo B, que se utilizan para redes de tamaño mediano que tienen entre 2^{8} (256) y 2^{16} anfitriones, asignan 14 bits al campo netid y 16 al hostid.
- Las direcciones tipo C, que se utilizan para redes de tamaño pequeñas que tienen menos de 2^{8} anfitriones, asignan 21 bits al campo netid y sólo 8 bits al hostid.[2]

Nótese que las direcciones IP se han definido de tal forma que es posible extraer rápidamente los campos netid o hostid. Los ruteadores, que utilizan el campo netid de una dirección para decidir a dónde enviar un paquete, dependen de una extracción eficiente para lograr una velocidad alta.

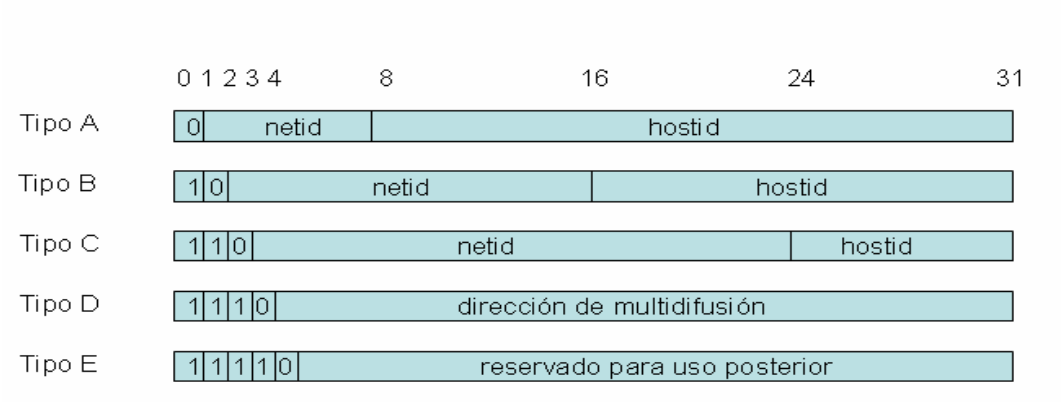


Figura 1. Las cinco formas de direcciones de Internet (IP).

[2] Para mayor información a cerca de los tipos D y E, consultar en el libro **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura.

2.1.3 LAS DIRECCIONES ESPECIFICAN CONEXIONES DE RED

Para simplificar e análisis, dijimos que una dirección de red de redes identifica un anfitrión, pero esto no es del todo preciso. Considere un ruteador que conecta dos redes físicas. No Podemos asignar una sola dirección IP si dicha dirección codifica un identificador de red así como un identificador de anfitrión. Cuando computadoras convencionales tienen dos o más conexiones físicas se les llama *anfitriones multi-homed*. Los anfitriones multi-homed y los ruteadores requieren de muchas direcciones IP. Cada dirección corresponde a una de las conexiones de red de las máquinas. Referirnos a los anfitriones multi-homed nos lleva a la siguiente consideración:

> *Debido a que las direcciones IP codifican tanto una red y un anfitrión en dicha red, no especifican una computadora individual, sino una conexión a la red.*

Por lo tanto, un ruteador que conecta cierto número de redes tiene cierto número de direcciones IP distintas, una para cada conexión de red.

2.1.4 DIRECCIONES DE RED Y DE DIFUSIÓN

Las direcciones de red de redes se pueden utilizar para referirse a redes así como a anfitriones individuales.[3]

Por regla, una dirección que tiene todos los bits del campo hostid igual a 0, se reserva para referirse a la red en sí misma.

[3] Para profundización consultar el libro, **Gallo, Michael. Hancock, William.** Comunicaciones Entre Computadoras y Tecnología de Redes.

Las direcciones IP se pueden utilizar para especificar la difusión; estas direcciones se transforman en difusión por hardware, si ésta se encuentra disponible. Por regla una dirección de difusión tiene todos los bits del campo hostid asignados como 1.

2.1.4.1 DIFUSIÓN DIRIGIDA.

Técnicamente la dirección de difusión que describimos se conoce como *dirección de difusión dirigida*,[4] debido a que contiene una identificación válida de red como el campo hostid de difusión. Una dirección de difusión dirigida se puede interpretar como ambigüedades en cualquier punto de una red de redes ya que identifica de forma única la red objetivo, además de especificar la difusión en dicha red. Las direcciones de difusión dirigidas proporcionan un mecanismo poderoso (y a veces algo peligroso) que permite que un sistema remoto envíe un solo paquete que será publidifundido en la red especificada.

Desde el punto de vista del direccionamiento, la mayor desventaja de la difusión dirigida es que requiere un conocimiento de la dirección de red.

2.1.4.2 DIFUSIÓN LIMITADA

Esta dirección de difusión también es llamada *dirección de difusión en red local*, esta proporciona una dirección de difusión para la red local, independientemente de la dirección IP asignada. La dirección de difusión

[4] Para profundización consultar el libro, **Gallo, Michael. Hancock, William.** Comunicaciones Entre Computadoras y Tecnología de Redes.

local consiste en treinta y dos 1s (unos).[5] Un anfitrión puede utilizar la dirección de difusión limitada como parte de un procedimiento de arranque antes de conocer su dirección IP o la dirección IP de la red local. Sin embargo, una vez que el anfitrión conoce la dirección IP correcta para la red local, tiene que utilizar la difusión dirigida.

Como regla general, los protocolos TCP/IP restringen la difusión al menor número posible de máquinas.

2.1.5 INTERPRETACION DE CERO

De igual manera como un campo consistente en 1s puede interpretarse como “todos”, como en “todos los anfitriones” de una red. En general el software de red de redes interpreta los campos que consisten en ceros (0s) como si fuera “esto”. La interpretación aparece a lo largo de la literatura. Por lo tanto, una dirección IP con campo hostid 0 se refiere a este anfitrión, y una dirección de redes con el ID de red de 0 se refiere a “esta” red.

2.2 RUTEO IP

Todos los servicios de red de redes utilizan un sistema de conexión de entrega de paquetes y también que la unidad básica de transferencia en una red de redes TCP/IP es el datagrama IP. Aquí proporcionaremos gran información sobre el servicio sin conexión, pues se describe como los

[5] Por esto es llamada también dirección de difusión “todos 1s”.

ruteadores que direccional datagramas IP y cómo los entregan en su destino final. En esta descripción de ruteo presentaremos los aspectos operacionales.

2.2.1 RUTEO EN UNA RED DE REDES

En un sistema de comunicación de paquetes, el ruteo es el proceso de selección de un camino sobre el que se mandarán paquetes y el ruteador es la computadora que hace la selección. El ruteo ocurre a muchos niveles. Por ejemplo, dentro de una red de área amplia que tiene muchas conexiones físicas entre computadores de datos, la red por sí misma es responsable de rutear paquetes desde que llegan hasta que salen. Este ruteo interno está completamente contenido dentro de la red de área amplia. Las máquinas en el exterior no pueden participar en las decisiones, sólo ven la red como una entidad que entrega paquetes.

Recuerde que el objetivo del IP es proporcionar una red virtual que comprenda muchas redes físicas, así como ofrecer un servicio sin conexión de entrega de paquetes. Por lo tanto, nos enfocaremos en el *ruteo en red de redes o ruteo IP*.[6] De forma análoga al ruteo dentro de una red física, el ruteo IP selecciona un camino por el que se debe enviar un datagrama. El algoritmo de ruteo IP debe escoger cómo enviar un datagrama pasando por muchas redes físicas.

[6] Los fabricantes también utilizan los términos *direccionamiento IP y conmutación IP* para describir el *ruteo IP*.

El ruteo en una red de redes puede ser difícil, en especial entre computadoras que tienen muchas conexiones físicas de red. De forma ideal, el software utilizado para el ruteo examinaría aspectos como la carga de la red, la longitud del datagrama o el tipo de servicio que especifica en el encabezado del datagrama, para seleccionar el mejor camino. Sin embargo, la mayor parte del software de ruteo IP es mucho menos sofisticado y selecciona rutas basándose en suposiciones sobre los caminos más cortos.

Para entender con mayor claridad el ruteo IP, debemos conocer la arquitectura de una red de redes TCP/IP. Lo primero que debemos saber es que una red de redes se compone de muchas redes físicas interconectadas por computadores conocidos como ruteadores. Cada ruteador tiene conexiones directas hacia dos o más redes. En contraste, por lo general un anfitrión se conecta directamente a una red física. Sin embargo, sabemos que es posible tener un anfitrión multi-homed conectado directamente a muchas redes.[7]

Tanto los anfitriones como los ruteadores participan en el ruteo de datagramas IP que viajan a su destino. Cuando un programa de

[7] Para mayor información a cerca de los anfitriones o host, consultar en el libro **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura.

aplicación en un anfitrión intenta comunicarse, los protocolos TCP/IP eventualmente generan uno o dos datagramas. El anfitrión debe tomar una decisión de ruteo cuando elige a dónde enviar los datagramas. Como se muestra en la figura 2, los anfitriones deben tomar decisiones de ruteo, inclusive si sólo tienen una conexión de red.

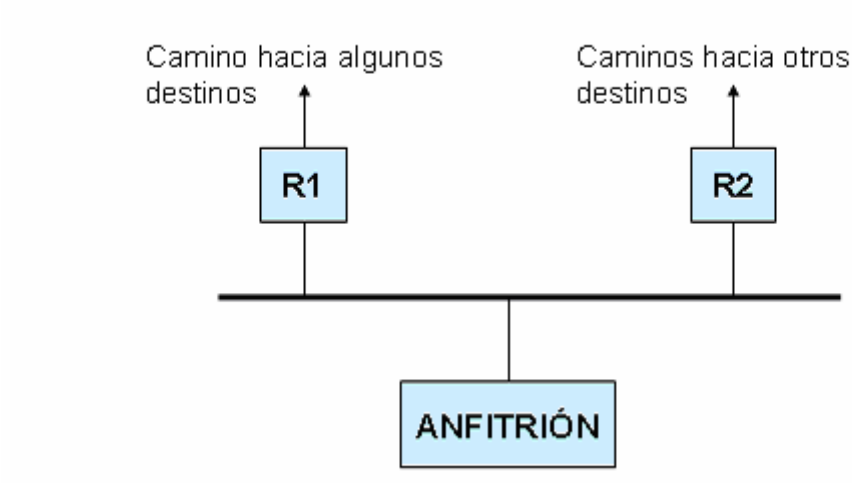


Figura 2. Ejemplo de un anfitrión singly-homed que debe rutear datagramas.

En el ejemplo anterior el anfitrión debe enviar un datagrama al ruteador R1 o al ruteador R2, ya que cada uno proporciona el mejor camino hacia algunos destinos.

Lógicamente los ruteadores también toman decisiones de ruteo IP.[8] Cualquier computadora con muchas conexiones de red puede actuar como ruteador y, como veremos, los anfitriones multi-homed que ejecutan el TCP/IP tienen todo el software necesario para el ruteo. Además, los sitios que no pueden adquirir ruteadores por separado a veces utilizan

[8] Principal propósito y razón para llamarlos *ruteadores.*

máquinas de tiempo compartido y propósito general como anfitriones y ruteadores.[9] Sin embargo, los estándares

TCP/IP hacen una gran diferenciación entre las funciones de un anfitrión y las de un ruteador en una solo máquina, a veces, encuentran que sus anfitriones multi-homed llevan a cavo interacciones inesperadas. Por ahora, nos concentraremos en distinguir los anfitriones de los ruteadores y asumiremos que los primeros no realizan la función, exclusiva de los ruteadores, de transferir paquetes de una red a otra.

2.2.2 ENTREGA DIRECTA E INDIRECTA

El ruteo podemos dividirlo en dos partes: *entrega directa* y *entrega indirecta*. La entrega directa, que es la transmisión de un datagrama desde una máquina a través de una sola red física hasta otra, es la base de toda la comunicación en una red de redes. Dos máquinas solamente pueden llevar a cabo la entrega directa si ambas se conectan directamente al mismo sistema subyacente de transmisión física (por ejemplo, una sola Ethernet). La entrega indirecta ocurre cuando el destino no es una red conectada directamente, lo que obliga al transmisor a pasar el datagrama a un ruteador para su entrega.

[9] Esta práctica por lo general se ve limitada a los sitios en universidades

2.2.2.1 ENTREGA DE DATAGRAMAS SOBRE UNA SOLA RED

Una máquina en una red física puede enviar una trama física directamente a otra máquina. Para transferir un datagrama IP, el transmisor encapsula el datagrama dentro de una trama física, transforma la dirección IP de destino en una dirección física de hardware y utiliza la red para entregar el datagrama. [10]

Para mayor facilidad de comprensión *la transmisión de un datagrama IP entre dos máquinas dentro de una sola red física no involucra ruteadores.*

El transmisor sabe si el destino reside en una red directamente conectada. Las direcciones IP se dividen en un prefijo específico de red y un sufijo específico de anfitrión. Para averiguar si un destino reside en una de las redes directamente conectadas, el transmisor extrae la porción de red de la dirección IP de destino y la compara con la porción de red de su propia dirección IP. Si corresponden, significa que el datagrama se puede enviar de manera directa. Una de las ventajas del esquema de direccionamiento de Internet es que la comprobación de que una máquina se puede alcanzar directamente, es muy eficiente.

Desde la perspectiva de una red de redes, la forma más fácil de pensar en la entrega directa es como el paso final de cualquier transmisión de datagramas, aún si el datagrama atraviesa muchas redes y ruteadores

[10] Envío de la trama resultante directamente a su destino.

intermedios. El último ruteador del camino entre la fuente del datagrama y su destino siempre se conectará directamente a la misma red física que la máquina de destino. Por lo tanto, el último ruteador entregará el datagrama utilizando la entrega directa. Podemos pensar en la entrega directa entre la fuente y el destino como un caso especial de ruteo de propósito general en una ruta directa, el datagrama nunca pasa a través de ningún ruteador intermedio.

2.2.2.2 ENTREGA INDIRECTA

La entrega indirecta es mucho mas fácil que la directa ya que el transmisor debe identificar un ruteador para enviar el datagrama. Luego, el ruteador debe encaminar el datagrama hacia la red de destino.

Para visualizar cómo trabaja el ruteo indirecto, imagínense una gran red con muchas redes interconectadas por medio de ruteadores, pero sólo con dos anfitriones en sus extremos más distantes. Cuando un anfitrión quiere enviar un datagrama a otro, lo encapsula y lo envía hacia el ruteador más cercano. Sabemos que se puede alcanzar un ruteador utilizando debido a que todas las redes físicas están interconectadas, así que debe existir un ruteador conectado a cada una. Por lo tanto, el anfitrión de origen puede alcanzar un ruteador utilizando una sola red física. Una vez que la trama llega al ruteador, el software extrae el datagrama encapsulado, y el software IP selecciona el siguiente ruteador a lo largo del camino hasta el destino. De nuevo, se coloca el datagrama

en una trama y se envía a través de la siguiente red física hacia un segundo ruteador, y así sucesivamente hasta que se pueda entregar de forma directa.

"Un enrutador sabe a dónde enviar cada datagrama y Un anfitrión sabe qué ruteador utilizar para llegar a un destino determinado."

Este enunciado lo explicaremos de la siguiente manera:

Ruteo IP controlado por tabla

Ruteo con salto al siguiente

2.2.3 RUTEO IP CONTROLADO POR TABLA

El algoritmo usual de ruteo IP emplea una tabla de *ruteo Internet*[11] en cada máquina que almacena información sobre posibles destinos y sobre cómo alcanzarlos. Debido a que tanto los ruteadores como los anfitriones rutean datagramas, ambos tienen tablas de ruteo IP. Siempre que el software de ruteo IP en un anfitrión necesita transmitir un datagrama consulta la tabla de ruteo para decidir a dónde enviarlo.

Si cada tabla de ruteo contuviera información sobre cada posible dirección de destino, sería imposible mantener actualizadas. A demás como el número de destinos posibles es muy grande, las máquinas no tendrían suficiente espacio para almacenar la información.[12]

[11] Conocida como tabla de ruteo IP

[12] Consultar **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP.

De manera conceptual, nos gustaría utilizar el principio de ocultación de información y permitir a las máquinas tomar decisiones de ruteo con mínima información. Por ejemplo, nos gustaría aislar la información sobre anfitriones específicos de ambiente local en el que existen y hacer que las máquinas que estén lejos ruteen paquetes hacia ellos sin saber dichos detalles. Por fortuna, el esquema de direccionamiento IP nos ayuda a lograr este objetivo. Recuerde que las direcciones IP se asignan de tal manera que todas las máquinas conectadas a una red física compartan un prefijo en común.[13] Ya hemos visto que una asignación de este tipo hace que la comprobación para la entrega directa sea eficiente. También significa que las tablas de ruteo sólo necesitan contener prefijos de red y no direcciones IP completas.

2.2.4 RUTEO CON SALTO AL SIGUIENTE

Utilizar la porción de red de una dirección de destino en vez de toda la dirección de anfitrión hace que el ruteo sea eficiente y mantiene reducidas las tablas de ruteo. También es importante, porque ayuda a ocultar información al mantener los detalles de los anfitriones específicos confinados al ambiente local en el que operan. Por lo común una tabla de ruteo contiene pares (N, R), donde N es la dirección IP del “siguiente” ruteador en el camino hacia la red N. El ruteador N es conocido como el *salto siguiente* y la idea de utilizar una tabla de ruteo para almacenar un

[13] Porción de red de la dirección

salto siguiente para cada destino es conocida como *ruteo con salto al siguiente*. Por lo tanto, la tabla de ruteo en el ruteador R sólo especifica un paso a lo largo del camino de R a su red de destino; el ruteador no conoce el camino completo hacia el destino.

Es importante entender que cada registro en una tabla de ruteo apunta hacia un ruteador que se puede alcanzar a través de una sola red. Esto es que todos los ruteadores listados en la tabla de ruteo de la máquina M deben residir en las redes con las que M se conecta de manera directa. Cuando un datagrama está listo para dejar M, el software IP localiza la dirección IP de destino y extrae la porción de red. Luego, M utiliza la porción de red para tomar una decisión de ruteo, seleccionando un ruteador que se pueda alcanzar directamente.

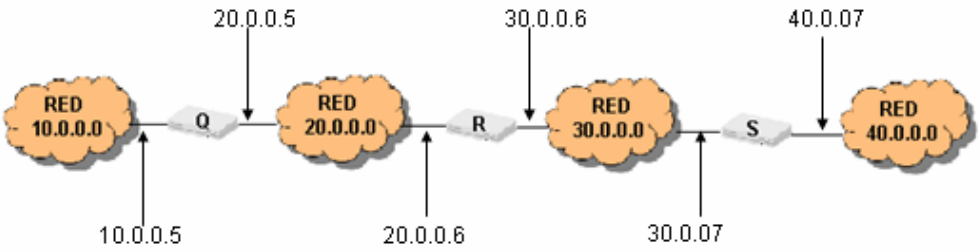
En la práctica, también aplicamos el principio de ocultación de información a los anfitriones. Insistimos que, aunque los anfitriones tengan tablas de ruteo IP, deben guardar información mínima en ellas. La idea es obligar a los anfitriones a que deleguen la mayor parte de sus funciones de ruteo a los ruteadores.[14]

En la figura 3 se muestra un ejemplo concreto que nos ayuda a explicar las tablas de ruteo.

La red de redes ejemplificada consiste en cuatro redes conectadas por tres ruteadores. En la figura 3 la tabla de ruteo proporciona las rutas que utiliza el ruteador R. Ya que R se conecta de manera directa a las redes

[14] Para profindizar, consultar en: **Doyle, Jeff. DeHaven, Jerrnifer. CISCO SYSTEMS.** Routing TCP/IP.

20.0.0.0 y 30.0.0.0, puede utilizar la entrega directa para llevar a cabo un envío a un anfitrión en cualquiera de esas redes. Teniendo un datagrama destinado para un anfitrión en la red 40.0.0.0, R lo rutea a la dirección 30.0.0.7, que es la dirección del ruteador S. Luego, S entregará el datagrama en forma directa. R puede alcanzar la dirección 30.0.0.7 debido a que tanto R como S se conectan directamente con la red 30.0.0.0.



(a)

Para alcanzar los anfitriones en la red	Rutear a esta dirección
20,0,0,0	Entregar directamente
30,0,0,0	Entregar directamente
10,0,0,0	20,0,0,5
40,0,0,0	30,0,0,7

(b)

Figura 3. (a) Ejemplo de una red con 4 redes y 3 ruteadores, y (b) tabla de ruteo en R.

Como se muestra en la figura 3, el tamaño de la tabla de ruteo depende del número de redes en la red; solamente crece cuando se agregan nuevas redes. Sin embargo, el tamaño y contenido de la tabla son independientes del número de anfitriones individuales conectados a las redes.

Para mayor comprensión resumimos el principio adyacente:

Para ocultar información, mantener reducidas las tablas de ruteo y tomar las decisiones de ruteo de manera eficiente, el software de ruteo IP sólo puede dar información sobre las direcciones de las redes de destino, no sobre las direcciones de anfitriones individuales.[15]

Escoger rutas basándose tan sólo en la identificación de la red de destino tiene muchas consecuencias. Primero, en la mayor parte de las implantaciones, significa que todo el tráfico destinado a cierta red toma el mismo camino. Como resultado, aún cuando existen muchos caminos, quizá no se utilicen constantemente. De igual manera, todos los tipos de tráfico siguen el mismo camino sin importar el retraso o la generación de salidas de las redes físicas. Segundo, debido a que el último ruteador del camino intenta comunicarse con el anfitrión final, solamente el ruteador puede determinar si el anfitrión existe o está en operación. Por lo tanto, necesitamos encontrar una forma para que el ruteador envíe reportes sobre problemas de entrega, de vuelta a la fuente original. Tercero,

[15] Consultado en **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura. Tercera edición

debido a que cada ruteador rutea el tráfico de forma independiente, los datagramas que viajan del anfitrión A al B pueden seguir un camino totalmente distinto a los que siguen los datagramas que viajan del anfitrión B al A. Necesitamos asegurarnos de que los ruteadores cooperen para garantizar que siempre sea posible la comunicación bidireccional.

2.2.5 RUTAS ASIGNADAS POR OMISIÓN

Otra técnica utilizada para ocultar información y mantener reducido el tamaño de las tablas de ruteo, es asociar muchos registros a un ruteador asignado por omisión. La idea es hacer que el software de ruteo IP busque primero la tabla de ruteo para encontrar la red de destino. Si no aparece una ruta en la tabla, las rutinas de ruteo envían el datagrama a un *ruteador asignado por omisión.*

El ruteo asignado por omisión es de gran ayuda cuando un sitio tiene pocas direcciones locales y sólo una conexión con el resto de la red de redes. Por ejemplo, las rutas asignadas por omisión trabajan bien en máquinas anfitriones que se conectan a una sola red física y alcanzan sólo un ruteador, que es la puerta hacia el resto de la red de redes. Toda la decisión de ruteo consiste en dos comprobaciones: una de la red local, y un valor asignado por omisión que apunta hacia el único ruteador posible. Inclusive si el sitio sólo contiene unas cuantas redes locales, el

ruteo es sencillo ya que consiste en pocas comprobaciones de las redes locales, más un valor asignado por omisión para todos los demás destinos.

2.2.6 RUTAS POR ANFITRION ESPECÍFICO

Aunque hemos dicho que todo el ruteo está basado en redes y no en anfitriones individuales, la mayor parte del software de ruteo IP permite que se especifiquen rutas por anfitrión como caso especial. Tener rutas por anfitrión le da al administrador de red local un mayor control sobre el uso de la red, le permite hacer comprobaciones y también se puede utilizar para controlar el acceso por razones de seguridad. Cuando se depuran conexiones de red o tablas de ruteo, la capacidad para especificar una ruta especial hacia una máquina individual resulta ser especialmente útil.

2.2.7 EL ALGORITMO DE RUTEO IP

Tomando en cuenta todo lo que hemos dicho, el algoritmo de ruteo IP es como sigue en la figura 4.[16]

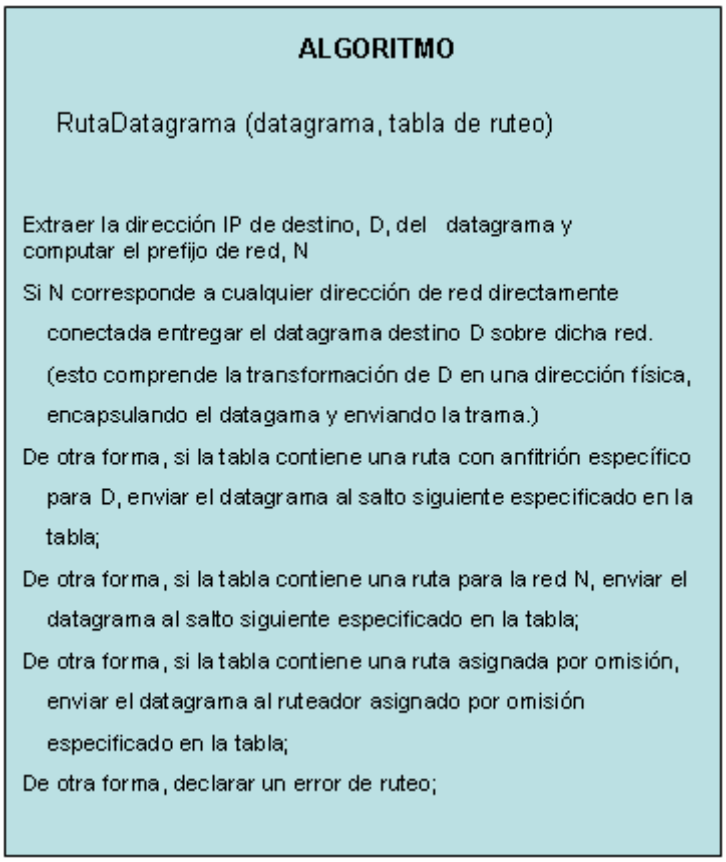


Figura 4. Por medio de un datagrama IP y una tabla de ruteo, este algoritmo selecciona el salto siguiente al que s e debe enviar el datagrama. Todas las rutas deben especificar un salto siguiente que resida en una red conectada directamente.[17]

[16] Consultado en **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura. Tercera edición
[17] Algoritmo que utiliza IP para direccional un datagrama.

2.2.8 RUTEO CON DIRECCIONES IP

Es importante entender que, a excepción de la disminución del tiempo de vida y de volver a computar la suma de verificación, el ruteo IP no altera el datagrama original. En particular, las direcciones de origen y destino del datagrama permanecen sin alteración; éstas siempre especifican la dirección IP de la fuente original y la dirección IP del último destino.[18]

Cuando el IP ejecuta el algoritmo de ruteo, selecciona una nueva dirección IP, que es la dirección IP de la máquina a la que a continuación se tendrá que enviar el datagrama. La nueva dirección es parecida a la dirección de un ruteador. Sin embargo, si el datagrama se puede entregar directamente, la nueva dirección será la misma que la del último destino.

Sabemos que la dirección IP seleccionada por el algoritmo de ruteo IP se conoce como la dirección de *salto al siguiente,* pues indica a dónde se tiene que enviar después el datagrama (aunque quizá no sea el último destino). El IP no almacena la dirección del salto siguiente en el datagrama; no existe un lugar reservado para ella. De hecho, el IP no *almacena* la información del salto siguiente. Después de ejecutar el algoritmo de ruteo, el IP pasa el datagrama y la dirección del salto siguiente al software de interfaz de red, responsable de la red física sobre la que el datagrama se debe enviar. El software de interfaz de red transforma la dirección física, pone el datagrama en la porción de datos

[18] La única excepción ocurre cuando el datagrama contiene una opción de ruta de origen.

de la trama y envía el resultado. Luego de utilizar la dirección de salto siguiente para encontrar una dirección física, el software de interfaz de red la descarta.

Puede parecer extraño que las tablas de ruteo almacenen la dirección IP del salto siguiente para cada red de destino cuando dichas direcciones se tienen que traducir a sus direcciones físicas correspondientes, antes de que se pueda enviar el datagrama. Si nos imaginamos un anfitrión que envía una secuencia de datagramas a la misma dirección de destino, la utilización de direcciones IP nos parecería muy ineficiente. El IP fácilmente extrae la dirección de destino en cada datagrama y utiliza la tabla de ruteo para producir una nueva dirección de salto siguiente. Luego pasa el datagrama y la dirección de salto siguiente a la interfaz de red, que recomputa la asignación para obtener una dirección física. Si la tabla de ruteo utilizó direcciones físicas, la transformación entre la dirección IP de salto siguiente y la dirección física se pueden llevar a cabo sólo una vez, evitando así cómputos innecesarios.

Existen dos razones importantes para que el software IP evite la utilización de direcciones físicas cuando almacena y computa las rutas, como podemos observar en la figura 5.[19]

[19] Consultado en: **Stallings, William.** Comunicación y Redes de Computadores. Séptima edición.

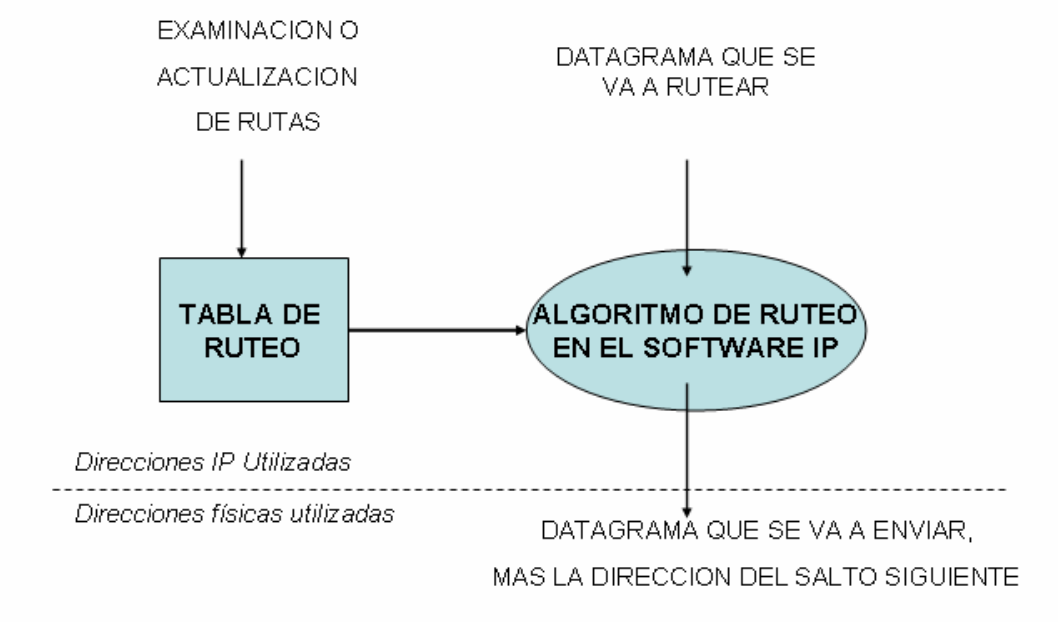


Figura 5. El software IP y la tabla de ruteo que utiliza, residen arriba de la frontera de dirección. Utilizar sólo direcciones IP facilita la examinación o cambios de las rutas y oculta los detalles de las direcciones físicas.

Primero, la tabla de ruteo proporciona una interfaz muy transparente en el software IP que rutea datagramas y el software de alto nivel que manipula las rutas. Para depurar problemas de ruteo, los administradores de red a menudo necesitan examinar las tablas de ruteo. La utilización de direcciones IP solamente en la tabla de ruteo facilita que los administradores las entiendan, lo mismo que ver dónde el software actualizó correctamente las rutas. Segundo, todo el sentido del protocolo Internet es construir una abstracción que oculte los detalles de las redes subyacentes.

En la figura 5, se muestra la *frontera de direcciones*, importante división conceptual entre el software de bajo nivel que entiende las direcciones

físicas y el software interno que solo utiliza direcciones de alto nivel. Arriba de esta frontera, se puede escribir todo el software para que se comunique utilizando direcciones de red de redes; el conocimiento de las direcciones físicas se relega a unas cuantas rutinas de bajo nivel. Veremos que, al respetar la frontera, también se facilita la comprensión, prueba y modificación de la implantación de los restantes protocolos TCP/IP.

2.2.9 MANEJO DE LOS DATAGRAMAS ENTRANTES

Hasta ahora, hemos analizado y comprendido el ruteo IP al describir cómo se toman las decisiones sobre los paquetes salientes. Sin embargo, debe quedar claro que el software también tiene que procesar los datagramas entrantes.

Cuando un datagrama IP llega a un anfitrión, el software de interfaz de red lo entrega al software IP para su procesamiento. Si la dirección de destino del datagrama corresponde a la dirección IP del anfitrión, el software IP del anfitrión acepta el datagrama y lo pasa al software de protocolo de alto nivel apropiado, para su procesamiento posterior, si la dirección IP de destino no corresponde, se requiere que el anfitrión descarte el datagrama (por ejemplo, está prohibido que los anfitriones intenten direccionar datagramas que accidentalmente se rutearon a la máquina equivocada).[20]

[20] Consultado en: **Stallings, William.** Comunicación y Redes de Computadores. Séptima edición.

A diferencia de los anfitriones, los ruteadores sí realizan el direccionamiento. Cuando llega un datagrama IP a un ruteador, este lo entrega al software IP. De nuevo surgen dos casos: que el que el datagrama haya podido llegar a su destino final o que probablemente necesite viajar más. Como con los anfitriones, si la dirección de destino del datagrama corresponde a la dirección IP, el software IP pasa el datagrama a un software de protocolo de nivel más alto para su procesamiento.[21] Si el datagrama no ha llegado a su destino final, el IP lo rutea utilizando el algoritmo estándar así como la información en la tabla local de ruteo.

La determinación sobre si un datagrama IP alcanzó su destino final no es tan insignificante como parece. Recordemos que hasta un anfitrión puede tener muchas conexiones físicas, cada una con su propia dirección IP. Cuando llega un datagrama IP, la máquina debe comparar la dirección de destino de red de redes con la dirección IP de cada una de sus conexiones. Si alguna corresponde, guarda el datagrama y loa procesa. Una máquina también debe aceptar datagramas que se transmitieron por difusión en la red física, si su dirección IP de destino es la dirección IP de difusión limitada, o es la dirección IP de difusión dirigida para esa red. Las direcciones de subred y de multidifusión hacen que el reconocimiento de direcciones sea aún más complejo. De cualquier forma, si la dirección no corresponde a ninguna de las direcciones de la máquina local, el IP

[21] Por lo general, los únicos datagramas destinados para un ruteador, son los utilizados para probar la conectividad o los que llevan comandos de manejo del ruteador.

disminuye el campo de tiempo de vida en el encabezado del datagrama, descartándolo si el contador llega a cero o computa una nueva suma de verificación y rutea el datagrama si la cuenta es positiva.

Todas las máquinas deben direccionar los datagramas IP que reciben debido a que un ruteador debe direccionar datagramas entrantes ya que esa es su función principal. También hemos dicho que algunos anfitriones multi-homed actúan como ruteadores, aunque realmente son sistemas de computación multi-propósito. Aunque utilizar un anfitrión como ruteador por lo general no es buena idea, si se elige utilizarlos de esa manera, el anfitrión debe configurarse para rutear datagramas al igual que lo hace un ruteador. Pero los anfitriones que no están diseñados o configurados para realizar esta actividad, no deberían rutear los datagramas que reciban, sino descartarlos.

Existen cuatro razones por las que un anfitrión que no esté diseñado para trabajar como ruteador debe abstenerse de realizar cualquier función de ruteo.

1. Cuando un anfitrión, de los ya mencionados, recibe un datagrama diseñado para alguna otra máquina, es porque algo salió mal con el direccionamiento, ruteo o entrega en la red de redes. El problema puede no verse si el anfitrión toma una acción correctiva al rutear el datagrama.
2. El ruteo causará tráfico innecesario de red.[22]

[22] puede quitarle tiempo a la CPU para utilizar de forma legítima el anfitrión.

3. Los errores simples pueden causar un caos. Suponga que cada anfitrión rutea tráfico e imagine lo que pasa si una máquina accidentalmente transmite por difusión un datagrama que está destinado al anfitrión H. debido a que se llevó a cabo una difusión, cada anfitrión dentro de la red recibe una copia del datagrama. Cada anfitrión direcciona su copia hacia H, que se verá bombardeado con muchas copias.
4. Los ruteadores hacen mucho más que rutear el tráfico, ellos utilizan unos protocolos especiales para reportar errores y los anfitriones no.[23]Los ruteadores también propagan información de ruteo para asegurarse de que sus tablas están actualizadas. Si los anfitriones rutean datagramas sin participar por completo en todas las funciones de ruteo, se pueden presentar anormalidades inesperadas.

2.3 SISTEMAS AUTÓNOMOS (AS)

El rompecabezas sobre el cual los ruteadores deben comunicar información de accesibilidad para los sistemas de núcleo se presenta debido a que hemos considerado únicamente la mecánica de la arquitectura de ruteo en una red de redes y no hemos considerado los aspectos administrativos. Las interconexiones, como las que se muestran

[23] Para evitar que muchos reportes de error saturen una fuente.

en la figura 6, que aparecen cuando una localidad en la columna vertebral de la red tiene una compleja estructura local, no deben ser pensadas como una red independiente múltiple, conectada hacia una red de redes, sino como una organización única que tiene múltiples redes bajo su control. Dado que las redes y los ruteadores se encuentran bajo una sola autoridad administrativa, esta autoridad puede garantizar que las rutas internas se mantengan consistentes y viables; más aún, la autoridad administrativa puede seleccionar a una de sus máquinas para servir como la máquina que aparecerá ante el mundo exterior como el acceso hacia la red. En la figura 6, dado que los ruteadores R2, R3 y R4 están bajo el control de una autoridad administrativa se puede arreglar que R3 anuncie la accesibilidad para las redes 2, 3 y 4.[24]

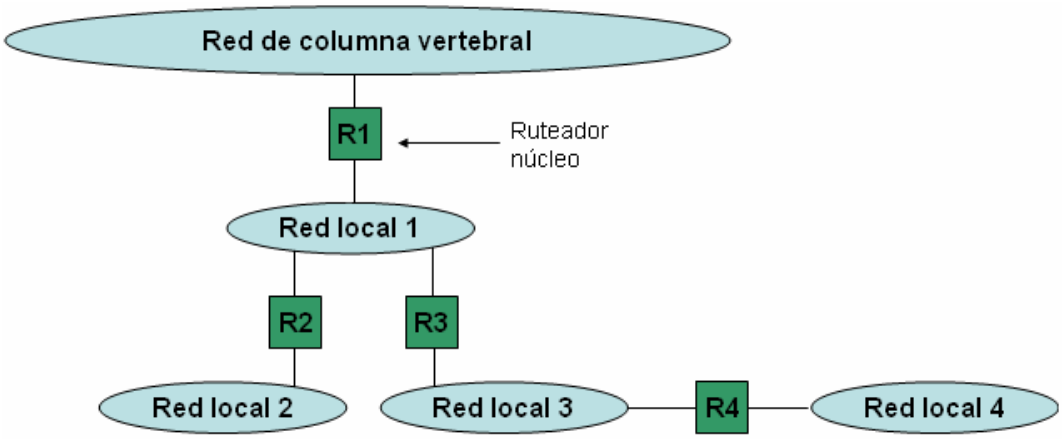


Figura 6. Múltiples redes con una sola conexión de columna vertebral de red.

[24] Asumimos que el sistema de núcleo ya tiene conocimiento sobre la red 1, ya que un ruteador núcleo está conectado directamente a ésta.

Para propósitos de ruteo a un grupo de redes y ruteadores controlados por una sola autoridad administrativa se le conoce como ***sistema autónomo*** *(AS)*. Los ruteadores dentro de una AS son libres de seleccionar sus propios mecanismos de exploración, propagación validación y verificación de la consistencia de las rutas. Nótese que bajo esta definición el ruteador núcleo en sí forma un AS.

Conceptualmente la idea de un AS es consecuencia directa y natural de la generalización de la arquitectura descrita en la figura 6, con AS reemplazando redes de área local. La figura 7 ilustra la idea.

Para lograr que las redes ocultas dentro de un AS sean accesibles a través de Internet, cada AS debe acordar la difusión de la información de la accesibilidad de la red hacia otros AS. Aún cuando los anuncios puedan ser enviados hacia cualquier AS, en una arquitectura de núcleo es crucial que cada AS difunda información hacia un ruteador núcleo. Usualmente un ruteador en un AS tiene la responsabilidad de anunciar rutas e interactuar de manera directa con uno de los ruteadores núcleo. Es posible, sin embargo, tener varios ruteadores y que cada uno anuncie un subconjunto de redes.

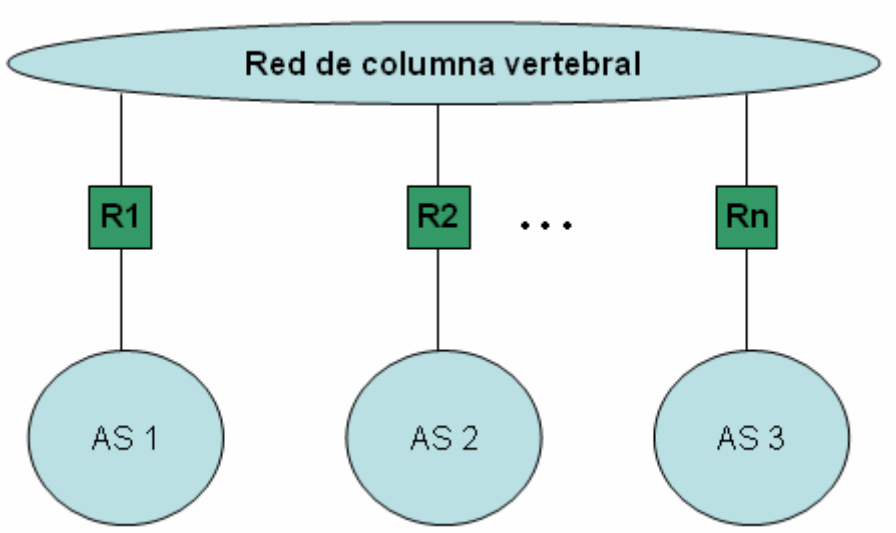


Figura 7. Arquitectura de una red de redes con AS en localidades de la columna vertebral de red.[25]

Un AS tiene la libertad para seleccionar una arquitectura de ruteo interna, pero debe reunir información sobre todas sus redes y designar uno o más tuteadotes que habrán de transferir información de accesibilidad hacia otros AS. Debido a que la conexión de Internet se vale de una arquitectura de núcleo, todos los AS deben transferir información de accesibilidad hacia los ruteadores núcleo de Internet.[26]

[25] Cada AS, está formado por varias redes y ruteadores bajo una sola autoridad administrativa.
[26] **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura.

3. PROTOCOLOS DE RUTEO

3.1 DEFINICIÓN DE PROTOCOLO

Los protocolos son reglas y procedimientos para la comunicación. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.[27]

3.2 CLASES DE PROTOCOLO

Existen dos grandes clases de protocolos, los internos y los externos.

A dos ruteadores que intercambian información de ruteo se les llama *vecinos exteriores*, si pertenecen a dos AS diferentes, *vecinos interiores* si pertenecen al mismo AS.

Los protocolos que emplean vecinos exteriores para difundir la información de accesibilidad a otros AS se le conoce como ***Protocolo de Pasarela Exterior (Exterior Gateway Protocol)* o *EGP*** y los ruteadores que se utilizan aquí se les conocen como *ruteadores exteriores.*

De igual manera ocurre con los protocolos que emplean vecinos internos, estos se les conoce como ***Protocolos de Pasarela Interior (Interior Gateway Protocol) o IGP*** y los ruteadores utilizados aquí se les conoce como ruteadores internos.

[27] Definición buscada en Internet en: http://es.wikipedia.org/wiki/protocolo"

3.2.1 PROTOCOLO DE PASARELA INTERIOR (IGP)

Hace referencia a los protocolos usados dentro de un AS. Los protocolos IGP más utilizados son ***RIP*** y ***OSPF***. Dos de los principales protocolos son RIP (que implementa el vector a distancia) y OSPF (es un protocolo de estado de enlace, esto es, que mantiene un mapa de la topología de las redes). IGP es usado dentro de una organización o dentro de los sitios de las organizaciones.

3.2.1.1 RUTEO EN UN SISTEMA AUTÓNOMO (AS)

3.2.1.2 RUTAS INTERIORES DINÁMICAS Y ESTÁTICAS

A dos ruteadores dentro de un AS se les llama *interiores* con respecto a otro. Por ejemplo, dos ruteadores núcleo Internet son interiores en comparación con otro debido a que el núcleo forma un solo AS. Dos ruteadores en un campus universitario son considerados interiores con respecto a otros mientras las máquinas en el campus estén reunidas en un solo AS. En redes de redes pequeñas que cambian lentamente, los administradores pueden establecer y modificar rutas a mano. El administrador tiene una tabla de redes y actualiza la tabla si una red nueva se añade o se elimina del AS. Por ejemplo, consideremos la red de redes de la pequeña corporación mostrada en la figura 8. el ruteo para

cada red de redes es insignificante porque sólo existe una ruta entre cualquiera de los dos puntos. El administrador puede configurar manualmente las rutas en todos los anfitriones y ruteadores. Si la red de redes cambia, al administrador debe reconfigurar las rutas en todas las máquinas.

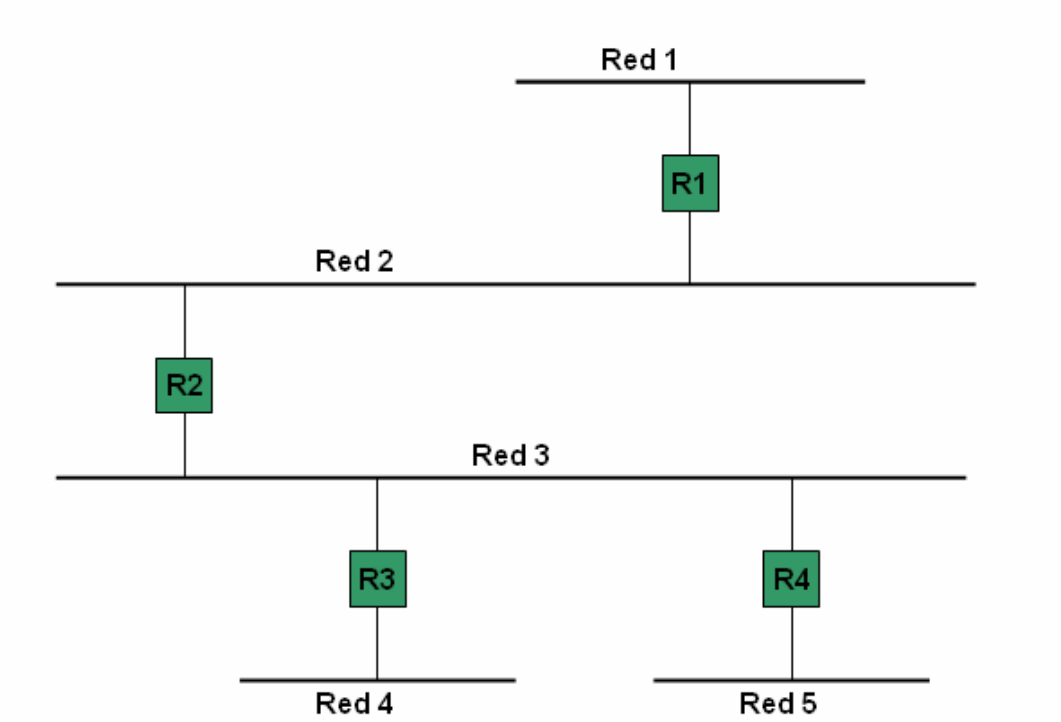


Figura 9. Ejemplo de una pequeña red de redes, formada por 5 redes Ethernet y 4 ruteadores en una sola localidad. Solo puede existir un ruteador entre cualquiera de los dos anfitriones en esta red de redes.[28]

[28] **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura.

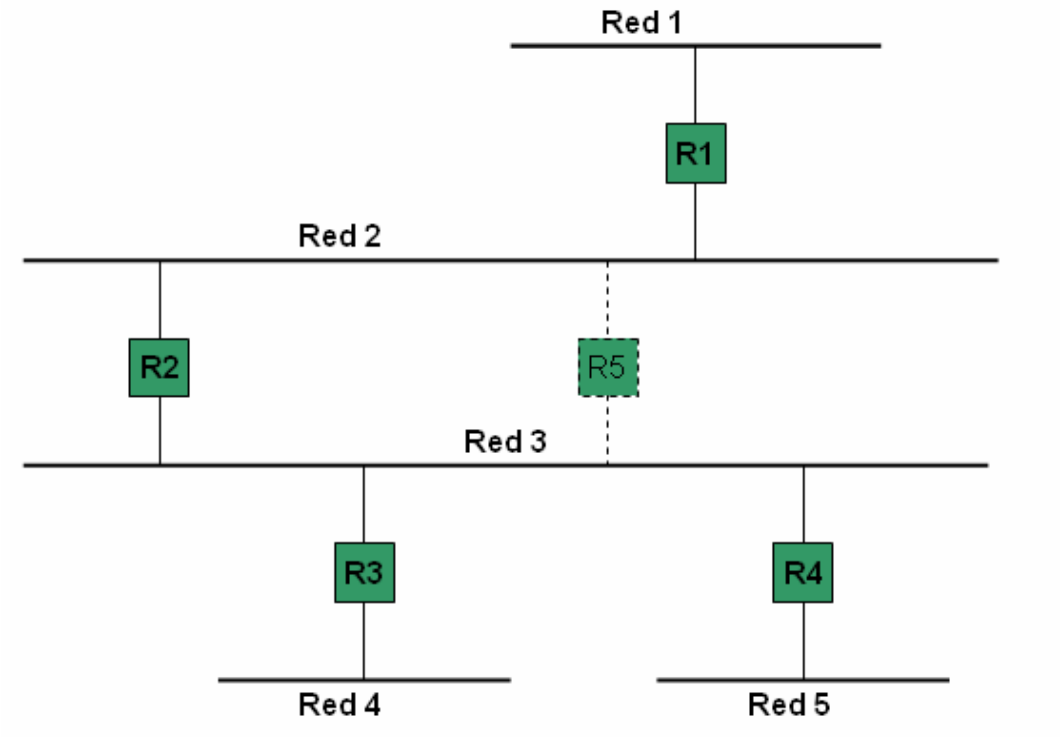


Figura 10. La adición del ruteador R5 introduce una ruta alterna entre las redes 2 y 3.[29]

Dado que no se trata sólo de un estándar, utilizaremos el término *protocolo de pasarela interno* o IGP, como una descripción genérica para referirnos a cualquier algoritmo que utilicen ruteadores interiores cuando intercambian información sobre accesibilidad de red y ruteo.

La figura 11, ilustra un AS que utiliza un IGP para difundir accesibilidad entre ruteadores interiores. En esta figura, IGP1 se remite al protocolo de

[29] El software de ruteo puede adaptarse rápidamente a una falla y conmutar rutas automáticamente hacia trayectorias alternas.

ruteador interior utilizado dentro del AS1, e IGP2 se remite al protocolo utilizado dentro del AS2. La figura también ilustra una idea importante:

Un solo ruteador puede utilizar 2 diferentes protocolos de ruteo simultáneamente, uno para la comunicación al exterior del AS y otro para la comunicación al interior de AS.

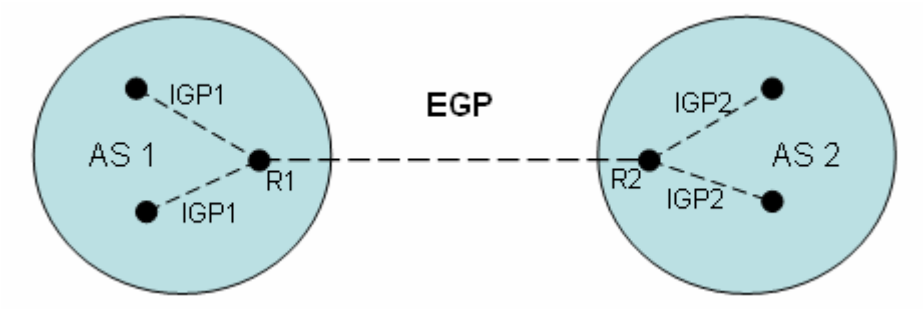


Figura 11. Representación del concepto de dos AS, cada uno utiliza su propio IGP internamente, pero se vale del EGP para realizar la comunicación entre un ruteador exterior y el otro AS.

En particular, los ruteadores que corren el EGP para anunciar accesibilidad por lo general necesitan correr también un IGP para obtener información desde el interior del AS.[30]

[30] **Comer, Douglas.** Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura.

3.2.2 PROTOCOLO DE PASARELA EXTERNO (EGP)

En la conexión de Internet, el EGP es especialmente importante ya que los AS o emplean para difundir información de accesibilidad hacia el sistema del núcleo.

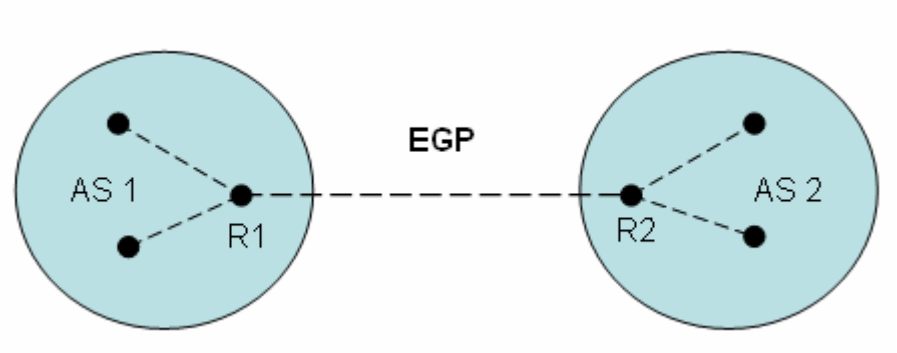


Figura 12. Ilustración conceptual de dos ruteadores exteriores, R1 y R2, que utilizan el EGP para anunciar redes en sus AS luego de reunir la información.[31]

En la figura 12 vemos que el ruteador R1 recoge información acerca de las redes en el AS1 y reporta esta información al ruteador R2 mediante el EGP, mientras el ruteador R2 reporta información desde el AS2.

El EGP tiene tres características principales:

[31] Los ruteadores exteriores por lo general están ubicados cerca de la orilla de un AS.

1. Soporta un mecanismo de adquisición de vecino que permite a un ruteador solicitar a otro un acuerdo para que los dos comuniquen información de accesibilidad. Decimos que un ruteador consigue un par EGP *(EGP peer)* o un vecino EGP. Los pares EGP son vecinos sólo en el sentido en que éstos intercambian información de ruteo, con lo cual no se hace alusión a su proximidad geográfica.
2. Un ruteador prueba continuamente si su vecino EGP está respondiendo.
3. Los vecinos EGP intercambian información de accesibilidad de red de manera periódica, transfiriendo un *mensaje de actualización de ruteo.*[32]

[32] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

4. PROTOCOLO DE INFORMACIÓN DE RUTEO (RIP)

Uno de los IGP más ampliamente utilizados es el *Protocolo de Información de Ruteo (RIP, Routing Information Protocol)*.[33] El software routed fue originalmente diseñado en la universidad de Berkeley en California para proporciona información consistente de ruteo y accesibilidad entre las máquinas de su red local. Este se apoya en la difusión de red física para realizar el intercambio de ruteo rápidamente. No fue diseñado para usarse en redes de área amplia.[34]

Con base en las primeras investigaciones de enlaces de redes realizadas en la corporación Xerox en el Centro de Investigación de Palo Alto (PARC), el routed implementa un protocolo derivado del *Protocolo de Información de Ruteo NS* de Xerox, pero se generalizó para cubrir varias familias de redes.

Al margen de mejoras menores con respecto a sus predecesores, la popularidad de RIP, como un IGP, no reside en sus méritos técnicos. Por el contrario, es el resultado de que Berkeley distribuyó el software routed junto con su popular sistema 4BSD de Unix. Así muchas localidades TCP/IP adoptaron e instalaron routed y comenzaron a utilizar RIP sin conocer sus méritos o limitaciones técnicas. Una vez instalado y corriendo, se convirtió en la base del ruteo local y varios grupos de investigadores lo adoptaron para redes amplias.

[33] Conocido también con el nombre de un programa que lo implementa, *routed*.
[34] En estos momentos si puede usarse para redes amplias

Posiblemente el hecho más sorprendente relacionado con el RIP es que fue construido y adoptado antes de que se escribiera un estándar formal. La mayor parte de las implantaciones se deriva del código Berkeley, teniendo entre sus limitaciones para el entendimiento del programador detalles no documentados y sutilezas relacionadas con la interoperabilidad. Conforme aparecen nuevas versiones, surgen más problemas. Un estándar RFC aparecido en 1988 hizo posible que los vendedores aseguraran la interoperabilidad.

El protocolo subyacente RIP es consecuencia directa de la implantación del ruteo de vector-distancia para redes locales. En principio, divide las máquinas participantes en *activas y pasivas* (silenciosas). Los ruteadores activos anuncian sus rutas a los otros; las máquinas pasivas listan y actualizan sus rutas con base en estos anuncios, pero no anuncian. Sólo un ruteador puede correr RIP de modo activo; un anfitrión debe utilizar el modo pasivo.

Un ruteador que corre RIP de modo activo difunde un mensaje cada 30 segundos. El mensaje contiene información tomada de la base de datos de ruteo actualizada. Cada mensaje consiste de pares, donde cada par contiene una dirección de red IP y un entero que representa la distancia hacia esta red. RIP utiliza una *métrica de conteo de saltos* (*hop count metric)* para medir la distancia hacia un destino. En la métrica RIP, un ruteador define un salto[35] desde la red conectada directamente, dos

[35] algunos protocolos definen las conexiones directas con un costo cero.

saltos desde la red que está al alcance de otro ruteador, y así sucesivamente. De esta manera, el *número de saltos (number of hops)* o el *contador de saltos (hop count)* a lo largo de una trayectoria desde una fuente dada hacia un destino dado hace referencia al número de ruteadores que un datagrama encontrará en una trayectoria. Debe ser obvio utilizar el conteo de una trayectoria con un conteo de saltos igual a 3 que cruza tres redes Ethernet puede ser notablemente más rápido que una trayectoria con un contador de saltos igual a 2 que atraviesa 2 líneas seriales lentas. Para compensar las diferencias tecnológicas, muchas implantaciones RIP permiten que los administradores configuren artificialmente los contadores de saltos con valores altos cuando deban anunciar conexiones hacia redes lentas.

4.1 PARTICIPANTES EN MODO ACTIVO Y PASIVO

Las interredes TCP/IP se basan en la premisa de que las puertas de enlace conocen las rutas correctas ya que intercambian entre sí la información de ruteo. En cambio, los anfitriones sólo conocen las rutas gracias a las puertas de enlace; la información de ruteo de los anfitriones puede no estar completa ni ser autorizada. De ahí que a los anfitriones se les prohíba informar a otras máquinas acerca de las rutas.

El protocolo RIP cumple esta regla ofreciendo dos modos básicos de operación. Los anfitriones usan RIP en modo pasivo, para escuchar pasivamente los mensajes RIP enviados por las puertas de enlace,

extraer de ellas información de ruteo y actualizar sus propias tablas de ruteo. El RIP pasivo no propaga información de la tabla local de ruteo. Las puertas de enlace usan RIP en modo activo. Los participantes activos escuchan los mensajes RIP de otras puertas de enlace, instalan nuevas rutas en sus tablas de ruteo y envían mensajes que contienen las entradas actualizadas de la tabla de ruteo así, los participantes activos se dedican a dos tareas (emisión y recepción, mientras que los pasivos sólo se dedican a una (recepción). Las siguientes secciones se enfocan en los participantes activos.

4.2 ALGORITMO VECTOR-DISTANCIA (BELLMAN-FORD)

El término vector-distancia indica una clase de algoritmos utilizada para difundir información de ruteo. La idea detrás de los algoritmos de vector-distancia es muy sencilla. El ruteador establece una lista de todas las rutas conocidas en una tabla. Cuando arranca, un ruteador inicia esta tabla de ruteo para que contenga una entrada de información por cada red conectada directamente. Cada introducción en la red identifica una red de destino y establece una distancia hacia la red, por lo general medida en saltos. Por ejemplo, la figura 13 muestra el contenido inicial de la tabla en un ruteador conectado a dos redes.[36]

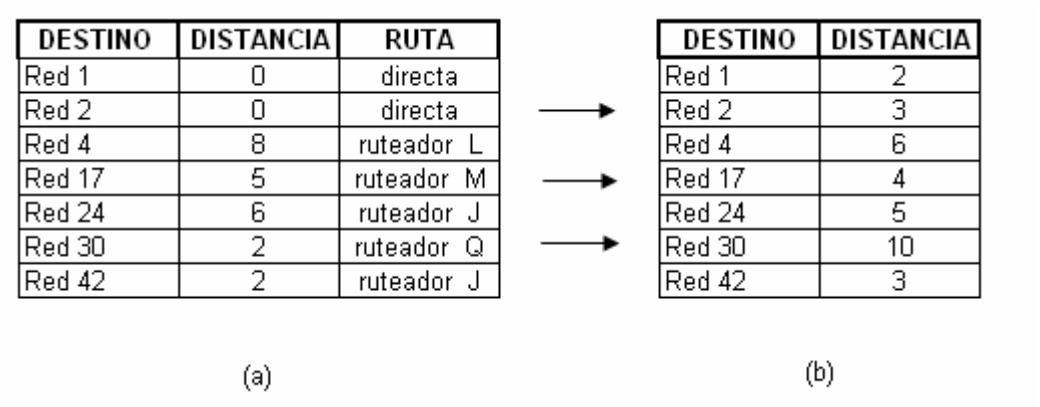
[36] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

DESTINO	DISTANCIA	RUTA
Red 1	0	directa
Red 2	0	directa

Figura 13. Tabla de ruteo inicial vector-distancia con una entrada de información para cada red conectada directamente. Cada entrada de la información contiene la dirección IP de una red y un número entero relacionado con la distancia hacia esa red.

Periódicamente cada ruteador envía una copia de su tabla de ruteo a cualquier otro ruteador que pueda alcanzar de manera directa. Cuando llega un reporte al ruteador K desde el ruteador J, K examina el conjunto de destinos reportados y la distancia de cada uno. Si J conoce una ruta más corta para alcanzar un destino o si J lista un destino que K no tiene en su tabla, o bien si K rutea actualmente hacia un destino a través de J y la distancia de J hacia el destino ha cambiado, K actualiza esta información en su tabla. Por ejemplo, la figura 14, muestra una tabla

existente en un ruteador K y un mensaje actualizado desde otro ruteador J.[37]



DESTINO	DISTANCIA	RUTA
Red 1	0	directa
Red 2	0	directa
Red 4	8	ruteador L
Red 17	5	ruteador M
Red 24	6	ruteador J
Red 30	2	ruteador Q
Red 42	2	ruteador J

(a)

DESTINO	DISTANCIA
Red 1	2
Red 2	3
Red 4	6
Red 17	4
Red 24	5
Red 30	10
Red 42	3

(b)

Figura 14. (a) Tabla de ruteo existente para un ruteador K, y **(b)** un mensaje entrante de actualización desde el ruteador J. Las entradas de información marcadas para actualizar se utilizarían para actualizar entradas de información existentes o añadir nuevas entradas a la tabla de K.

Obsérvese que si J reporta una distancia N, el dato actualizado en K tendrá la distancia N+1.[38] Por supuesto, la tabla de ruteo completa contiene una tercera columna que especifica una ruta. La entrada inicial de datos se marca con el valor *entrega directa (direct delivery).* Cuando el

[37] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

[38] La distancia para alcanzar el destino desde J, más la distancia para alcanzar J

ruteador K añade o actualiza una entrada de datos en respuesta al mensaje que proviene del ruteador J, asigna al ruteador J como la ruta para tal dato.

El término vector-distancia proviene del hecho de que la información se envía en mensajes periódicos. Un mensaje contiene una lista de pares (V,D), donde V identifica el destino (llamado vector) y D es la distancia hacia el destino. Nótese que el algoritmo vector-distancia reporta las rutas en primera persona (pensemos que un ruteador anuncia: “puedo alcanzar el destino V que está a la distancia D”). En este tipo de diseño, todos los ruteadores deben participar en el intercambio de información de vector-distancia para que las rutas sean eficientes y consistentes.

Aún cuando los algoritmos vector-distancia son fáciles de implementar, tienen desventajas. En un ambiente completamente estático, los algoritmos de vector-distancia difunden rutas hacia todos los destinos. Cuando las rutas cambian rápidamente, sin embargo, los cómputos podrían ser no estables. Cuando una ruta cambia (por ejemplo, si aparece una nueva conexión o si una conexión vieja falla), la información se propaga lentamente de un ruteador a otro. Esto significa que algunos ruteadores pueden tener información de ruteo incorrecta.

4.3 ALGORITMO RIP BÁSICO Y MÉTRICA DE COSTO

RIP usa un algoritmo vector-distancia ya mencionado con anterioridad, para propagar rutas y una difusión en redes locales para entregar

mensajes. Cada puerta de enlace difunde periódicamente las rutas de su tabla de ruteo IP actual a todas a todas las interfaces de red. Al igual que otros protocolos vector-distancia, el mensaje RIP contiene pares que consisten en una red de destino y la distancia hacia esa red.[39]

Cuando llega un mensaje de actualización RIP, la máquina receptora examina cada entrada y la compara con su ruta actual hacia el mismo destino, D. el receptor usa una desigualdad triangular para probar si la ruta notificada para D es superior a la ruta existente. Esto es cuando el receptor examina una entrada recibida por la puerta de enlace G, éste pregunta si el costo de ir a G, mas el costo de ir de G a D, es menor que el costo actual de ir a D. expresado en términos matemáticos, el receptor R se pregunta si

costo(R,G) + costo (G,D) < costo(R,D)

Costo (i,j) indica el costo de la trayectoria menos costosa de i a j. el receptor sólo actualiza la entrada de su tabla de ruteo cuando el costo de enviar el tráfico a través de la puerta de enlace G es menor que el actual. Cuando cambia una ruta, el receptor le asigna un costo igual a:

costo(R,G) + costo(G,D)

[39] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

Debido a que el costo de llegar a una puerta de enlace vecina es 1, el nuevo costo se convierte en

costo(R,D) = costo(G,D) +1

Aunque la explicación anterior parece sencilla, hay un detalle final que la complica. Supongamos que la ruta actual de R al destino D, pasa a través de la puerta de enlace G. cuando llega una actualización de G, R debe cambiar el costo de esta ruta, independientemente de que G reporte un aumento o una reducción del costo. Así la versión final de este algoritmo se convierte en:

Cuando de la puerta de enlace llega una actualización RIP con una métrica M para el destino D, compárela con la ruta actual. Si no existe ninguna ruta, créela con el siguiente salto igual a G y el costo igual a M+1. si la ruta actual especifica a G como el siguiente salto, defina el costo de la ruta como M+1. De otro modo, si el costo de la ruta actual es mayor que M+1, defina el costo como M+1 y establezca el siguiente salto a G.

4.4 INESTABILIDAD Y SOLUCIONES

4.4.1 CONTADOR AL INFINITO

La mayoría de los algoritmos vector-distancia comparte el mismo problema, ya que permiten bucles de ruteo temporales. Cuando dos o más puertas de enlace se bloquean en una secuencia circular, un bucle de ruteo se presenta para el destino D; de modo que cada puerta de enlace piensa que la trayectoria óptima para el destino D pasa por la siguiente puerta de enlace de la secuencia. Los bucles de ruteo más sencillos implican dos puertas de enlace, cada una de las cuales piensa que la otra es el siguiente mejor salto en la ruta hacia un destino determinado.

Las puertas de enlace que usan RIP no detectan fácilmente os bucles de ruteo. Cuando se presenta un bucle de ruteo hacia el destino D, el protocolo RIP hace que las puertas de enlace involucradas incrementen lentamente su métrica una a la vez. Esto continuará hasta que la métrica alcance un valor infinito, tan grande que el software de ruteo lo interpretará con el significado de que “no existe ninguna ruta hacia este destino”. Para ayudar a limitar los daños que causan los bucles de ruteo, RIP establece que el infinito es un número pequeño.

Para limitar el tiempo que pueda persistir un bucle de ruteo, RIP establece que el infinito es 16. Cuando la métrica de ruteo alcanza ese valor, RIP interpretará que el significado es que “no existe ninguna ruta”.

4.4.2 CAIDAS DE LA PUERTA DE ENLACE Y EXPIRACION DEL TIEMPO DE ESPERA DE LA RUTA

RIP requiere que todas las puertas de enlace y anfitriones participantes apliquen un tiempo de espera a todas las rutas. La ruta debe expirar cuando se vence el tiempo de espera. Para entender el tiempo de espera, considere lo que sucede cuando se cae una puerta de enlace G que ha participado activamente en RIP.[40] Las puertas de enlace vecinas han recibido mensajes de actualización de G y han instalado rutas que utilizan a G como su siguiente salto. Cuando G se cae, los vecinos no tienen forma de saber que la ruta que han seleccionado como su siguiente salto ha quedado invalidada. En esencia, el costo de la ruta se ha vuelto infinito, pero los vecinos no tienen forma de enterarse del cambio ya que la puerta de enlace responsable de difundir las actualizaciones de ruteo se ha caído. Así, las puertas de enlace que reciben información de RIP asumen la responsabilidad de asegurar que la ruta siga siendo correcta.

Cuando instale o cambie una ruta, asocie un temporizador a ella, si no llega información para revalidar la ruta antes de que expire el tiempo de espera, declare que la ruta es inválida.

4.4.3 HORIZONTE DIVIDIDO

Una de las causas más comunes de los bucles de ruteo surge cuando las puertas de enlace notifican toda la información de ruteo en todas las interfaces de la red. Para entender el problema, considere tres puertas de enlace A, B y C, conectadas a la misma Ethernet. Suponga que la puerta

[40] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

de enlace A tiene una trayectoria de costo 1 hacia el destino D, y la ha notificado difundiendo un paquete de actualización RIP. Tanto B como C reciben la actualización e instalan rutas hacia el destino D con costo 2. si ellas notifican sus rutas, no hay ningún problema pues son más costosas que la ruta que notifica A.

Ahora supongamos que se cae la puerta de enlace A. si B o C siguen notificando bastante tiempo su ruta a D de costo 2, las máquinas de la red llegarán a dar por expirada la ruta que notificaba A y adoptarán la ruta de costo 2. De hecho, en cuanto expira la ruta notificada por A, ya sea B o C adopta la ruta que notifica la otra, lo que crea un bucle temporal de ruteo. Para evitar lo bucles de ruteo, RIP aplica una técnica conocida como *horizonte dividido*. La regla es sencilla:

Cuando envíe una actualización RIP a través de una interfaz de red determinada, nunca incluya información de ruteo adquirida en esa interfaz.

Una forma de considerar esta regla es desde el punto de vista del ruteo que se presenta dentro de una puerta de enlace. Si una puerta de enlace G se enteró de una ruta hacia el destino D a través de la interfaz de la red N, entonces la ruta de G debe especificar el siguiente salto que yace en la red. Esto es, G rutea todos los datagramas dirigidos a D hacia una puerta de enlace N. Ahora supongamos que G incluye su ruta hacia el destino D cuando difunde una actualización RIP a través de una red N. si una puerta

de enlace o anfitrión de la red N no tiene ninguna ruta actual hacia D,[41] instala la ruta notificada y envía a G todos los datagramas dirigidos a D. si un datagrama dirigido a D llega a G, éste reenviará el datagrama al siguiente salto, que se encuentra en la red N. así, G reenvía nuevamente los datagramas que llegar por la red N a la misma red por la cual llegaron. El horizonte dividido resuelve el problema de bucles de ruteo, evitando las notificaciones que pueden causarlos.

4.4.4 POISON REVERSE

Esta técnica[42] modifica la técnica del horizonte dividido. En lugar de evitar la propagación de rutas fuera de la red desde la cual llegaron, esta técnica usa las actualizaciones para transportar información negativa.

Cuando envíe una actualización RIP a través de determinada interfaz de red, incluya todas las rutas, pero establezca la métrica en infinito para aquellas rutas adquiridas en esa interfaz.

Poison reverse romperá rápidamente los bucles de ruteo. Si cada una de dos máquinas tiene una ruta al destino D que apunta hacia la otra máquina, y si están configuradas para que envíen una actualización con el costo definido como infinito, se romperá el bucle en cuanto una máquina envíe su actualización.

Pero esto tiene una desventaja, y es que incrementa el tamaño de los mensajes de actualización (y por lo tanto consume más ancho de banda).

[41] Quizá porque haya ocurrido un error
[42] También llamada Horizonte Dividido con Poison Reverse.

Sin embargo para la mayoría de las puertas de enlace, el aumento de tamaño de los mensajes de actualización no causa problemas.

4.4.5 EXPIRACION DEL TIEMPO DE ESPERA DE LA RUTA CON POISON REVERSE

RIP requiere que las puertas de enlace establezcan un tiempo de espera para cada ruta y que la invaliden cuando expire el tiempo de espera. La implementación más obvia simplemente elimina una ruta de la tabla de ruteo cuando expira el temporizador. Sin embargo, cuando RIP usa la actualización poison reverse, no puede descartar rutas que se hayn vuelto inválidas. En cambio, debe llevar el registro de que la ruta existía y que ahora su costo es infinito.

RIP sólo necesita conservar las rutas que expiraron hasta el momento en que los mensajes de salida propaguen la información a las puertas de enlace vecinas. En principio RIP sólo necesita conservar una ruta expirada a lo largo de un ciclo de actualización.

4.4.6 ACTUALIZACIÓN ACTIVADAS

Esta técnica emplea actualizaciones rápidas para acelerar el proceso de convergencia después de un cambio.

Siempre que una puerta de enlace cambia la métrica de una ruta, debe enviar inmediatamente un mensaje de actualización a todas sus vecinas, sin esperar al ciclo de actualización.[43]

4.4.7 ALEATORIEDAD PARA EVITAR TORMENTAS DE DIFUSIÓN

El estándar del protocolo especifica que RIP debe hacer que la emisión de las actualizaciones activadas sea aleatoria.

Siempre que una puerta de enlace cambie la métrica de una ruta, debe enviar un mensaje de actualización a todas sus vecinas después de una breve demora aleatoria, pero sin esperar a la actualización periódica común.

Para entender en qué ayuda la demora aleatoria, recuerde que RIP usa difusión de hardware para entregar los mensajes de actualización, e imagine que varias puertas de enlace comparten una Ethernet. Piense en la actualización poison reverse. Siempre que una de las puertas de enlace envíe una actualización para un destino D, las demás puertas de enlace de la interfaz Ethernet instalarán el cambio, lo que activará actualizaciones.[44] Así, todas las puertas de enlace tratarán de difundir simultáneamente su actualización activada y se producirá una tormenta de difusión. De hecho, si el sitio decidiera adquirir todas sus puertas de enlace del mismo proveedor, éstas tendrían el mismo hardware y

[43] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

[44] Incluso una actualización poison reverse para la interfaz Ethernet a través de la cual llegó la información.

ejecutarían el mismo software, lo que las haría generar la respuesta activada exactamente al mismo tiempo. Para eliminar la emisión simultánea, RIP especifica que una puerta de enlace debe esperar un pequeño plazo aleatorio antes de enviar las actualizaciones activadas.

4.5 FORMATO DEL MENSAJE RIP

Los mensajes RIP pueden ser clasificados, a grandes rasgos, en dos tipos: mensajes de información re ruteo y mensajes utilizados para solicitar información. Ambos se valen del mismo formato, consistente en un encabezado fijo seguido por una lista opcional de pares de redes y distancias. La figura 15, mostramos el formato de los mensajes.

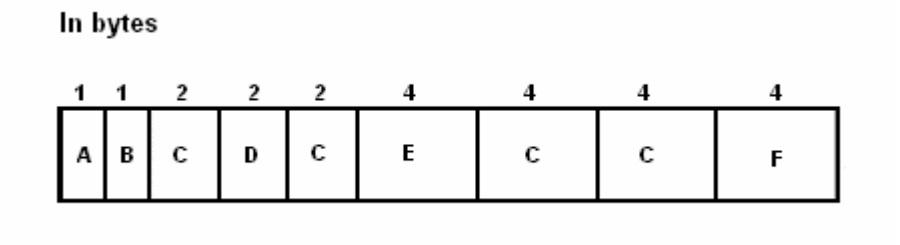


Figura 15. Formato de un mensaje RIP.

En la figura 15, notamos que dentro de cada cuadro hay una letra. Les mostraremos que significado tiene cada una de ella.[45]

A, *comando*, especifica una operación dentro de la siguiente tabla

COMANDO	SIGNIFICADO
1	Solicitud para información parcial o completa de ruteo
2	Respuesta con distancias de red de pares desde la tabla de ruteo del emisor
3	Activar el modo de trazado (obsoleto)
4	Desactivar el modo de trazado (obsoleto)
5	Reservado para uso interno de Sun Microsystems

Figura 16. Tabla de comando.

B. *versión*, este campo contiene el número de la versión del protocolo

C. *cero*, este campo corresponde a que siempre debe estar puesto a cero

D. *Familia de red,* indica la dirección de la familia de red.

E. *dirección IP de la red.* Especifica la dirección IP para la entrada

F. *métrica,* distancia hacia la red.

4.6 RIP (versión 2)

Por su diseño original, el RIP no soporta los conceptos de sistemas autónomos, subred, o autenticación. El RIP tampoco puede interpretar rutas BGP o EGP. Varias extensiones del protocolo original fueron

[45] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

incorporadas para ampliar su utilidad. Este protocolo, el RIP-2, mantiene el comando de RIP, número de versión, familia de red, dirección IP y los campos métricos. Los mensajes RIP-2 que llevan información en cualquiera de los campos no usados de la versión 1 tendrán un 2 en el campo de número de versión. El contenido del campo de dos bytes no usado en ambas versiones se ignora. Así un paquete RIP-2 no altera el contenido de RIP.

RIP-2 es un borrador. Su status es electivo[46]. Es menos potente que otros IGPs recientes tales como OSPF pero tiene las ventajas de una fácil implementación y menores factores de carga. La intención de RIP-2 es proporcionar una sustitución directa de RIP que se pueda usar en redes pequeñas y medianas, sobretodo, que pueda interoperar con RIP-1.

RIP-2 aprovecha que la mitad de los bytes de un mensaje RIP están reservados (deben ser cero) y que la especificación original estaba diseñada con las mejoras en la mente de los desarrolladores, particularmente en el uso del campo de versión. Un área notable en la que este no es el caso es la interpretación del campo de métrica. RIP-1 lo especifica con un valor de 0 a 16 almacenado en un campo de 4 *bytes.* Por compatibilidad, RIP-2 preserva esta definición, lo que significa en que interpreta 16 como infinito, y desperdicia la mayor parte del rango de este campo. [47]

[46] . Se describe en el RFC 1723. RIP-2 extiende RIP-1

[47] Consultado en http://www.ietf.org/ripv2.html

5. OSPF (ABRIR PRIMERO LA RUTA MÁS CORTA)

En 1988, el grupo: Fuerza de Trabajo de Ingenieros de Internet (IETF) empezó a desarrollar un nuevo protocolo de ruteo que reemplazaría al protocolo RIP. Se desarrollo entonces el protocolo de pasarela interior Primero el camino abierto más corto. OSPF es un protocolo de ruteo para redes IP que se basa en las especificaciones de RFC. En la década de los 90 OSPF fue recomendado como un protocolo de ruteo estándar.

En abril de 1990, la NASA cambió al protocolo OSPF y el tráfico de ruteo se redujo drásticamente. Tras un cambio e interrupción de la red, las informaciones de ruteo global se restablecían rápidamente (a los pocos segundos comparados con los minutos de otros protocolos más antiguos).

El protocolo del OSPF era desarrollado debido a una necesidad en la comunidad del Internet de introducir un protocolo interno no-propietario de la entrada de la alta funcionalidad (IGP) para la familia del protocolo de TCP/IP. La discusión de crear un IGP ínteroperable común para el Internet comenzó en 1988 y no consiguió formaliza hasta 1991. [48]

5.1 CONFIGURACIÓN Y OPCIONES OSPF

OSPF trata de abarcar una gran variedad de arquitecturas de interred y configuraciones de ruteo, el protocolo incluye varias alternativas. Por ejemplo, considere una interred en la que una línea serial conecta dos

[48] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición

puertas de enlace. La implementación convencional de IP trata a cada conexión como si fuera una red y requiere que la línea tenga asignada una dirección IP. Sin embargo, algunas implementaciones de IP conservan las direcciones de protocolo al permitir que dos puertas de enlace se comuniquen a través de una *conexión anónima*, una línea serial que no tiene dirección IP. A diferencia de la mayoría de los protocolos de ruteo, OSPF puede difundir información de ruteo tanto de conexiones anónimas como de conexiones convencionales.

La generalidad de OSPF tiene un costo: el protocolo es grande y complicado, por lo que su especificación puede ser difícil de entender. Aún más importante, para ser completamente general, el software OSPF debe estar diseñado de modo que pueda configurarse para una interred específica. En efecto, el protocolo contiene muchas variantes posibles y casos especiales. Por ejemplo, aunque OSPF está diseñado como un protocolo de puerta de enlace interior que se usa dentro de un AS, permite que el administrador de sistema particione el sistema autónomo en subconjuntos llamados áreas. Cada puerta de enlace debe estar colocada en una de estas áreas para que OSPF especifique como una puerta de enlace que se encuentra en el borde de un área y que transmite información de ruteo a una puerta de enlace que se encuentra en el borde de otra área.

Para entender OSPF sin enredarnos en las generalidades y los casos especiales, analizaremos por separado cada una de las funciones del protocolo

5.2 MODELO DE TEORÍA DE GRÁFICOS DE OSPF

Al igual que la mayoría de los algoritmos de estado de enlaces, OSPF usa un modelo de teoría de gráficos para la topología de red, el cual le permite calcular las rutas más cortas. Cada puerta de enlace difunde periódicamente información sobre el estado de sus conexiones con las redes; OSPF envía cada mensaje de estado a todas las puertas de enlace participantes. La puerta de enlace usa la información del estado de los enlaces para ensamblar un gráfico. Siempre que la puerta de enlace reciba información que modifique su copia del gráfico de topología (por ejemplo, cuando una conexión falla), ejecuta un algoritmo convencional de gráficos para calcular las rutas más cortas en el gráfico, y se basa en el resultado para crear una tabla de ruteo hacia el siguiente salto.

OSPF usa un gráfico para modelar una interred,[49] llamado también *gráfico de topología*. Cada nodo del gráfico de topología de OSPF corresponde, ya sea a una puerta de enlace o a unja red. Si existe una conexión física entre dos objetos de una interred, el gráfico OSPF contendrá un par de flechas (una en cada dirección) entre los dos nodos que representan los objetos por ejemplo la figura 17 muestra una conexión entre una puerta

[49] OSPF modela las conexiones de una interred.

de enlace y una red, así como las flechas en el gráfico correspondiente en el gráfico OSPF.[50]

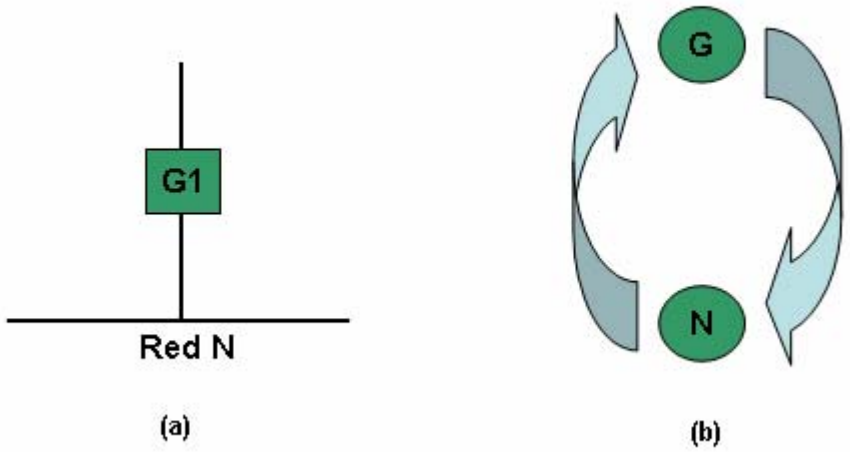


Figura 17. (a) conexión entre una puerta de enlace y una red; **(b)** el correspondiente par de flechas en el gráfico OSPF.

OSPF usa el término *red de multiacceso* para referirse a una red que conecta varias puertas de enlace.[51] El gráfico OSPF de una red de multiacceso consta de un nodo que representa a la red, un nodo por cada puerta de enlace y un par de flechas por cada conexión entre una puerta de enlace y la red. Por ejemplo la figura 18, muestra una red multiacceso con varias puertas de enlace conectadas y el gráfico OSPF correspondiente.

[50] Consultado en **Comer, Douglas** Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición
[51] Utilizando el algoritmo de Dijkstra, consultado http://www.javvin.com/algoritm /rfc1772.pdf

OSPF también permite que el gráfico modele una conexión anónima de punto a punto entre un par de puertas de enlace.

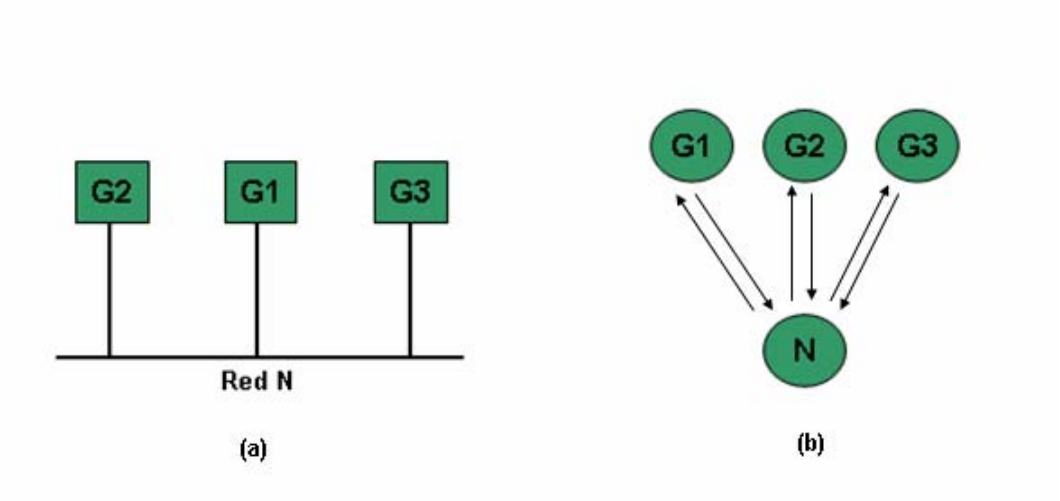


Figura 18. (a) Una red multiacceso con tres puertas de enlace conectadas y **(b)** el gráfico OSPF correspondiente a las tres conexiones.

Para modelar una conexión serial anónima, OSPF usa un par de flechas que conectan los nodos que representan a las dos puertas de enlace. De este modo, a diferencia del gráfico de la red de multiacceso, el gráfico de una conexión serial anónima contiene un nodo correspondiente a la línea serial.

Para permitir que las puertas de enlace calculen las rutas más cortas, cada flecha de un gráfico OSPF tiene asignado un *peso* que corresponde con el costo de esa ruta. Al configurar OSPF, el administrador de red asigna los pesos con un número positivo para cada interfaz de red. El costo asignado a una interfaz determinada puede ser elegido por razones administrativas o técnicas. Por ejemplo, un peso puede reflejar el costo monetario de usar la interfaz, el ancho de banda de red disponible a lo

largo de la interfaz o una política administrativa diseñada para fomentar o desalentar el uso de la interfaz.

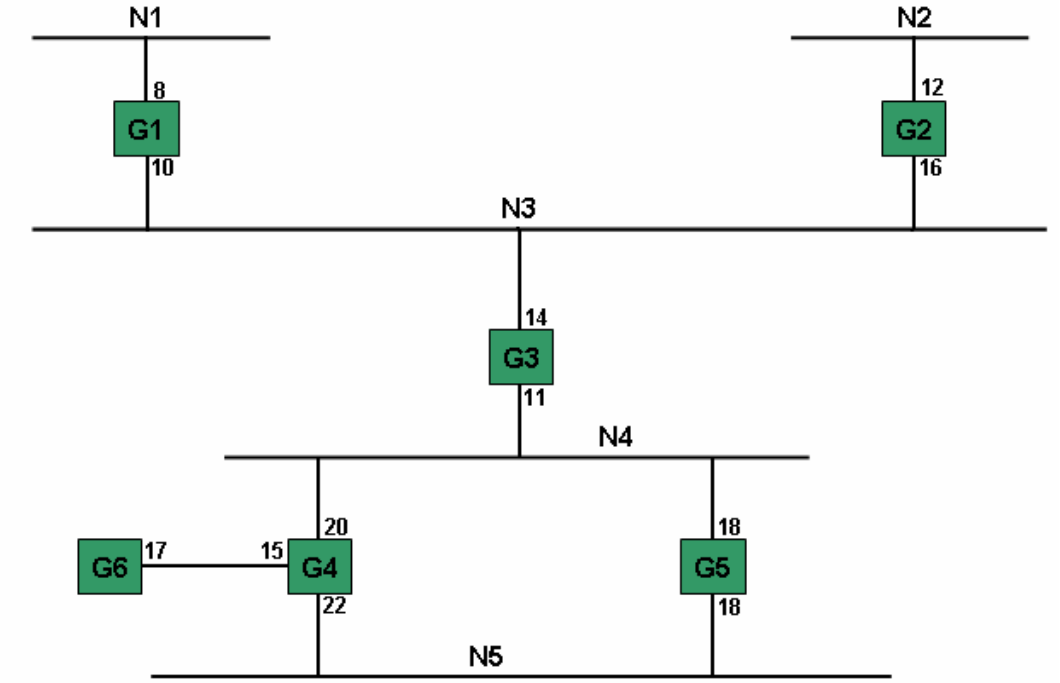


Figura 19. Red que contiene redes y puertas de enlace con costos asignados a cada interfaz

La figura 19 muestra una interred con costos asignados a cada interfaz.

Al igual que la mayoría de los algoritmos de ruteo, OSPF construye tablas de ruteo que reenvían los datagramas a lo largo de la ruta de menor costo. Así, aunque tanto la puerta de enlace G4 como la G5 de la figura 19, ofrecen conectividad a través de las redes N4 y N5, OSPF ruteará los datagramas a través de la puerta de enlace G5, ya que tiene asignado un costo menor. La figura 20 muestra el modelo gráfico OSPF de la misma interred de la figura 19. el gráfico contiene un nodo por cada puerta de enlace y un nodo por cada red de multiacceso. El gráfico no contiene un

nodo para la conexión anónima entre las puertas de enlace G4 y G6. en cambio, un par de flechas conectan directamente los nodos G4 y G6.

Como muestra la figura, cada flecha del gráfico OSPF que va de un nodo que representa una puerta de enlace a un nodo que representa una red, tiene asignado un peso igual al costo de usar la interfaz. Sin embargo, las flechas que van del nodo que representa una red al que representa una puerta de enlace tienen un peso de cero. La razón de la asignación asimétrica del peso es simple: la asociación de un peso independiente para una flecha que va del nodo de puerta de enlace al nodo red, permite un costo a cada conexión.

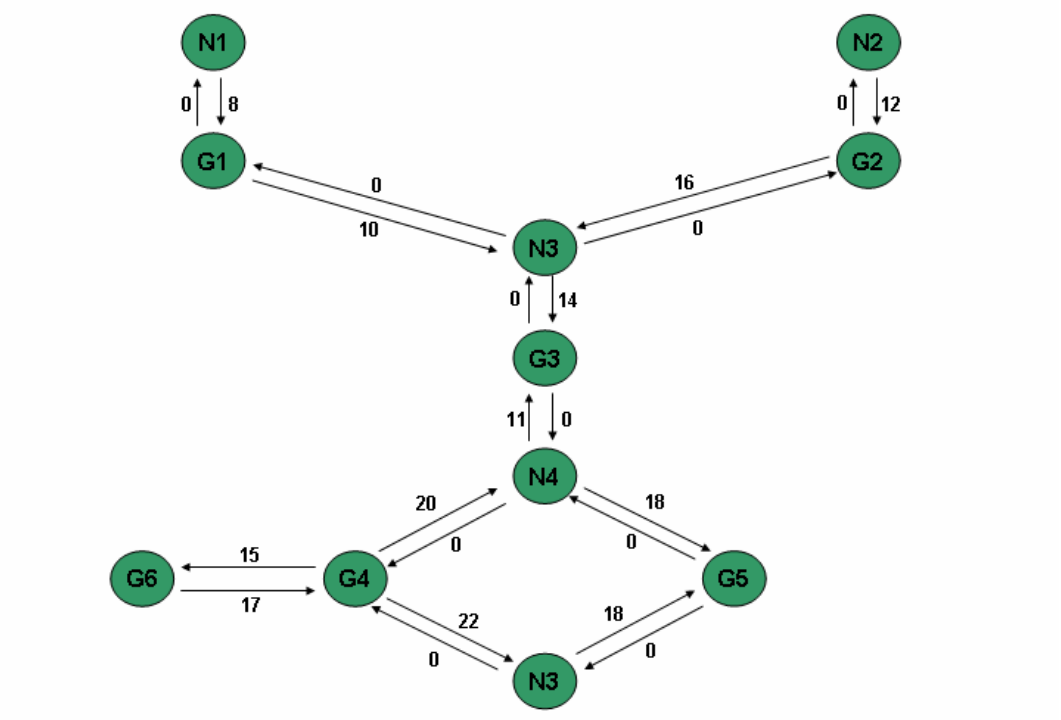


Figura 20. El gráfico OSPF de la interred de la figura 20. los números junto a las flechas del gráfico indican el peso asignado a la conexión de red que representan.

Un peso de cero en una flecha que va de un nodo de red a uno de puerta de enlace, garantiza que OSPF sólo contará una vez el costo a lo largo de una ruta de la red. De esta forma, el administrador puede ejercer control haciendo que el costo de acceder a una red determinada desde una puerta de enlace, sea mayor que acceder a la misma red desde otra puerta de enlace. Lo que es más, el peso de cero permite entender más fácilmente el costo, ya que da la posibilidad al administrador de sumar los costos a lo largo de una ruta desde el origen hasta el origen hasta el destino.

6. IGRP (Interior Gateway Routing Protocol)

IGRP es un protocolo de ruteo interno utilizado en TCP/IP y OSI.[52] Se considera un IGP (Interior Gateway Protocol) pero también ha sido utilizado como un protocolo de ruteo externo para el ruteo inter-dominio. IGRP utiliza el algoritmo del vector distancia. El concepto es que cada ruteador no necesita conocer todas las rutas/enlaces de la red entera. Cada ruteador, informa acerca de los destinos y su distancia correspondiente. Cada ruteador escuchando información, ajusta las distancias y las propaga a los ruteadores vecinos.[53]

La información sobre la distancia en IGRP está representada como una combinación de ancho de banda disponible, retardo, carga y fiabilidad del enlace. Esto permite conseguir rutas óptimas.

El protocolo de ruteo de Gateway Interior fue desarrollado por Cisco para enfrentar algunos problemas asociados con el ruteo de redes heterogéneas grandes. La diferencia clave entre el IGRP y el RIP es la métrica de ruteo.

IGRP trata temas relacionados con bucles de ruteo implementando los conceptos de horizonte partido y retención, similares a las implementaciones de los RIP.

[52] Protocolo creado por CISCO SYSTEMS.
[53] consultado en www cisco com-warp-public-459-bgp-toc

6.1 DESCRIPCIÓN IGRP

IGRP es un protocolo que asigna un número de ruteadores para coordinar su ruteo. Sus metas son:

- Ruteo estable incluso en redes muy grandes y complejas. No deben producirse bucles, incluso si son transitorios.
- Rápida respuesta a cambios en la topología de la red-
- Pequeño overhead, IGRP no usa más ancho de banda que lo que necesita para su tarea.
- Reparte el tráfico entre rutas paralelas diferentes cuando éstas son en términos generales igual de buenas.
- Toma en cuenta la tasa de errores y el nivel de tráfico en diferentes caminos
- La capacidad de manejar múltiples “tipos de servicio” con un conjunto simple de información.

La actual implementación de IGRP maneja ruteo para TCP/IP. De todos modos, el diseño básico esta propuesto para ser capaz de manejar una variedad de protocolos.

Ninguna herramienta va a resolver todos los problemas de ruteo. Generalmente el problema del ruteo se rompe en varias piezas.

Protocolos como IGRP son llamados “protocolos de ruteo interno” (IGPs). Están propuestos para su uso en un conjunto simple de redes, bajo una dirección simple o una estrecha coordinación de los directores. Estos conjuntos de redes son conectados por “protocolos de ruteo externo” (EGPs). Un IGP está diseñado para mantener gran cantidad de detalles sobre la topología de la red. Su prioridad es fija en producir rutas óptimas y respondiendo rápidamente a los cambios. Un EGP está destinado a proteger un sistema de redes contra errores o una intencionada astucia por otros sistemas. Su prioridad está en los controles de estabilidad y administrativos.

IGRP tiene algunas similitudes con viejos protocolos con Xerox’s Routing Information Protocol, Berkeley’s RIP, y Dave Mill’s Hello. Difiere con estos protocolos en que está diseñado para redes más grandes y complejas.

Como estos viejos protocolos, IGRP es un protocolo basado en el algoritmo del vector distancia. Los ruteadores intercambian información de ruteo solo con sus ruteadores vecinos. Esta información de ruteo contiene un resumen de información sobre el resto de la red. Cada ruteador solo necesita resolver parte del problema, y solo tiene que recibir una porción de los datos totales.

La principal alternativa es una clase de algoritmos referidos a SPF (shortest path first). Que están basados en la técnica de “flooding” (inundación), donde todo ruteador debe mantener información del estado

de toda interfase en todos los otros ruteadores. Cada ruteador independientemente resuelve el problema desde su punto de vista usando información de toda la red. En algunas circunstancias SPF puede ser capaz de responder a cambios más rápidamente. Para prevenir los bucles, IGRP tiene que ignorar nuevos datos durante unos pocos minutos después de fijar los cambios. Porque SPF tiene información directamente de cada uno de los ruteadores, es posible evitar estos bucles en el ruteo. Puede actuar con la nueva información inmediatamente. De todos modos, SPF tiene más información que IGRP, tanto en las estructuras de datos internas y como en los mensajes que intercambian los ruteadores. Las implementaciones de SPF tienen más overhead que las implementaciones de IGRP, en otras cosas son iguales.

6.2 EL PROBLEMA DEL IGRP

IGRP esta diseñado para usarse en ruteadores que conectan distintas redes. Asumimos que las redes usan la tecnología basada en paquetes. De hecho los ruteadores actúan como conmutadores de paquetes. Cuando un equipo conectado a una red quiere enviar un paquete a otro equipo en una red diferente, dirige el paquete al ruteador. Si el destino se encuentra en una de las redes conectadas al ruteador, el ruteador mandará el paquete al destino.[54] Sino lo enviará a otro ruteador que se

[54] Paquete enviado directamente dentro de un AS.

encuentre cerca del destino. Los ruteadores utilizan las tablas de rutas para ayudarse a decidir qué hacer con el paquete.

La principal propuesta de IGRP es permitir a los ruteadores construir y mantener las tablas de rutas.

6.3 METRICA UTILIZADA POR IGRP

La métrica utilizada por IGRP incluye:[55]

- El retardo de la topología
- El Ancho de Banda
- La ocupación de la línea
- La fiabilidad

El retardo de la topología es la cantidad de tiempo que pasa hasta llegar al destino a través de la ruta, asumiendo una red no cargada. Desde luego hay un retardo adicional cuando la red está cargada.

De todos modos, la carga se mide por la ocupación del canal, no intentando medir el retraso actual.

El ancho de banda de la ruta es simplemente el ancho de banda en bits por segundo del enlace más lento de la ruta.

[55] consultado en www_cisco_com-warp-public-459-bgp-toc

La ocupación de la línea indica cuánto de este ancho de banda está actualmente en uso. Éste es medido y cambiará con la carga.

La fiabilidad indica la actual tasa de error. Es una fracción de los paquetes que llegan al destino sin error. Se mide.

Aunque no son usadas como parte de la métrica, dos piezas de información adicionales son pasadas con ella: *la cuenta de saltos y la MTU (Maximun Transfer Unit)*.

El contador de saltos es simplemente el número de ruteadores que el paquete debe atravesar para llegar al destino deseado.

La MTU es el máximo tamaño de paquete que puede ser enviado a lo largo de todo el trayecto sin fragmentación. Es la mínima de las MTUs de todas las redes incluidas en la ruta al destino.

Basado en la información de la métrica, una simple “métrica compuesta” es calculada para la ruta. Esta métrica compuesta combina el efecto de varios componentes métricos en un número simple que representa lo buena que es la ruta. Esta métrica se usa para decidir la mejor ruta.

Cuando un ruteador es por primera vez encendido, su tabla de ruteo es inicializada. Esto, debe ser hecho por un operador desde un Terminal, o

bien leyendo la información desde los archivos de configuración. Se proporciona una descripción de cada red conectada al ruteador, incluyendo el retraso a través del enlace[56] y el ancho de banda del enlace.

6.3.1 NÚMERO MÁXIMO DE SALTOS

IGRP posee un número máximo de saltos de 255, que normalmente se establece más bajo que los 100 predeterminados. Dado que IGRP utiliza actualizaciones *flash*, contar hasta 100 no lleva mucho tiempo. No obstante, es preciso establecer el número máximo de saltos a algo menor, a no ser que tenga una red enorme. Deberá ser un número como mínimo igual de grande que el número máximo de *ruteadores* por los que una ruta tenga que pasar en la red. Si se intercambia el ruteo IGRP por una red externa, el número de saltos deberá incluir la red más esa red externa.

6.3.2 PROCESO DE CONSTRUCCIÓN DE TABLAS POR EL ALGORITMO DE BELLMAN – FORD.

El proceso básico de construcción de las tablas de routing por intercambio de información con los vecinos es descrito por el algoritmo de Bellman – Ford.[57]

[56] cuanto le cuesta a un bit atravesar el enlace
[57] consultado en www_cisco_com-warp-public-459-bgp-toc

En IGRP, el algoritmo general de Bellman-Ford es modificado en tres aspectos críticos:

En lugar de una métrica simple, un vector de métricas es utilizado para caracterizar la ruta. Una simple métrica compuesta puede ser computada a partir de este vector de acuerdo con la ecuación 1. El uso de un vector permite al ruteador acomodar diferentes tipos de servicio utilizando coeficientes distintos en la ecuación.1.

[(K1 /Be) + (K2 * Dc)] r **ecuación 1**

Donde:

K1, K2: constantes → indican el peso asignado al ancho de banda y al delay. Dependerán del "tipo de servicio"

Be: ancho de banda efectivo. Ancho de banda cuando la red no está cargada x (1 – ocupación del canal)

Dc: delay

r: (reliability) fiabilidad → % de transmisiones que son recibidas con éxito en el siguiente salto

En principio, Dc (composite delay), puede ser definido como:

Dc = Ds + Dcir + Dt

Donde:

Ds = switching delay

Dcir = delay del circuito (retardo de propagación de 1 bit)

Dt =retardo de transmisión

La ruta que minimice esta métrica será la mejor.

Cuando existe más de una ruta para un mismo destino, el ruteador puede rutear los paquetes por más de una ruta.[58]

Se dan 2 ventajas por utilizar un vector de información métrica:

Proporciona capacidad de soportar múltiples “tipos de servicio” desde el mismo conjunto de datos.

Precisión

Cuando se utiliza una métrica simple, normalmente se trata como si fuera un delay. Cada enlace en el camino es añadido a la métrica total. Si hay un enlace con un bajo ancho de banda, normalmente se representa por un gran delay.

En lugar de escoger la ruta con la métrica más pequeña, el tráfico es repartido entre diferentes rutas, cuyas métricas caen dentro de un

[58] consultado en www_cisco_com-warp-public-459-bgp-toc

determinado rango. Esto permite distintas rutas para ser utilizadas en paralelo, proporcionando un ancho de banda efectivo mayor que con una solo ruta. Una varianza V es especificada por el administrador de red. Todas las rutas con métrica mínima se mantienen. También, todas las rutas cuya métrica es menor que VxM se mantienen. El tráfico es distribuido a través de múltiples rutas en una proporción inversa a las métricas compuestas.

Diferentes características son introducidas para proporcionar estabilidad en situaciones donde la topología está cambiando. Estas características han sido propuestas para prevenir bucles en la topología y el problema de la cuenta a infinito. Las principales características de estabilidad son: “holddowns”, “triggered updates”, “split horizon”, and “poisoning”.

6.4 ACTUALIZACIONES IGRP

Un ruteador que ejecuta IGRP envía una difusión de actualización cada 90 segundos. Declara una ruta como inaccesible si no recibe una actualización del primer *ruteador* de la ruta dentro de tres periodos de actualización (270 segundos). Transcurridos siete periodos de actualización (630 segundos), el *ruteador* eliminará la ruta de la tabla de ruteo. IGRP utilizará la actualización *flash y la* actualización inversa para acelerar la convergencia del protocolo de ruteo.[59]

[59] Consultado en **Doyle, Jeff. DeHaven, Jerrnifer. CISCO SYSTEMS.** Routing TCP/IP.

El temporizador controla la frecuencia de los mensajes de actualización del ruteador. Una **actualización flash** es el envío de una actualización antes de que transcurra el intervalo de actualización periódica para advertir a otros ruteadores de un cambio en la métrica. Las actualizaciones inversas están previstas para eliminar grandes bucles de ruteo que estén causados por aumentos en la métrica de ruteo. Las actualizaciones inversas son enviadas para eliminar una ruta y colocarla en espera, con lo que se evita que se use la nueva información de ruteo durante un periodo de tiempo concreto.

6.5 ESTABILIDAD DE IGRP

IGRP proporciona una serie de características que están diseñadas para mejorar su estabilidad, entre las cuales se incluyen las siguientes:

- *Esperas.*
- *Horizontes divididos.*
- *Actualizaciones inversas.*

Estas características fueron descritas anteriormente.

7. (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL) EIGRP

EIGRP es un protocolo que combina las ventajas de los protocolos de ruteo por estado de enlace y de vector-distancia.

Los protocolos tradicionales de ruteo tienen que recalcular sus algoritmos antes de anunciar las rutas hacia fuera.

Se diseña para dar toda la flexibilidad de los protocolos de ruteo tales como OSPF pero con una convergencia mucho más rápida. Además, EIGRP tiene módulos Protocolo-Dependientes que puedan tratar de Appletalk y del IPX así como el IP.

La redistribución entre EIGRP y otros protocolos de ruteo es generalmente automática.

EIGRP es una versión realzada de IGRP. La misma tecnología del vector de la distancia encontró en IGRP también se utiliza en EIGRP, y sigue habiendo la información subyacente de la distancia sin cambiar. Las características de la convergencia y la eficacia de funcionamiento de este protocolo han mejorado perceptiblemente. Esto permite una arquitectura mejorada mientras que conserva la inversión existente en IGRP.

La tecnología de la convergencia se basa en la investigación conducida en SRI internacional. El algoritmo de la actualización que difunde (DUAL) es el algoritmo usado para obtener la lazo-libertad en cada instante a través de un cómputo de la ruta. [60]Esto permite todas las rebajadoras

[60] Algoritmo usado para obtener la lazo-libertad en cada instante a través de un cómputo de la ruta.

implicadas en un cambio de la topología para sincronizar en el mismo tiempo. Las rebajadoras que no son afectadas por los cambios de la topología no están implicadas en el recomputo. El tiempo de la convergencia con los rivales DUAL es que de cualquier otro ruteo existente protocolan.

EIGRP se ha ampliado para ser red-capa-protocolo independiente.

7.1 CONVERGENCIA RÁPIDA

EIGRP utiliza el Diffusing Update Algoritmo (DUAL) para conseguir una convergencia rápida. Un ruteador que ejecuta EIGRP almacena rutas de reserva, en la medida de lo posible, para los destinos, de forma que pueda adaptarse rápidamente a las rutas alternativas. Si no hay ruta apropiada o de reserva en la tabla de ruteo local, EIGRP consulta a sus vecinos para descubrir una ruta alternativa. Estas consultas se propagan hasta que se encuentra una ruta alterna.[61]

7.2 UTILIZACIÓN REDUCIDA DEL ANCHO DE BANDA

EIGRP no envía actualizaciones periódicas. En su lugar, utiliza actualizaciones parciales cuando cambia la métrica a un destino. Cuando cambia la información de ruta, DUAL envía una actualización sobre ese enlace, en vez de toda la tabla de ruteo. Además, la información sólo se

[61] Consultado en **Doyle, Jeff. DeHaven, Jerrnifer. CISCO SYSTEMS.** Routing TCP/IP.

pasa a los ruteadores que lo requieren, en contraste con el funcionamiento del protocolo del estado de enlace, que envía una actualización de cambio a todos los ruteadores de un área.

7.3 SOPORTE DE CAPA DE MÚLTIPLES REDES

EIGRP soporta AppleTalk, IP y Novell Netware, utilizando módulos que dependen del protocolo (PDM). EIGRP tiene sus raíces en el ruteo por vector-distancia. Al igual que su predecesor IGRP, EIGRP es muy fácil de configurar y es adaptable a una amplia gama de topologías de red. Lo que hace de EIGRP en protocolo de vector-distancia avanzado es la incorporación de varias características de estado de enlace, como el descubrimiento dinámico de vecinos.

Aunque EIGRP es compatible con IGRP, ofrece un rendimiento superior, gracias a una rápida convergencia que garantiza en todo momento una topología sin bucles. Las actualizaciones de ruteo parcial sólo se generan en los cambios de topología. La distribución de actualizaciones parciales está limitada, de forma que sólo se actualizan los *ruteadores* que necesitan la información. Como protocolo de ruteo sin clase, EIGRP publica una máscara de ruteo para cada red de destino.

Para resumir, a continuación se ofrecen las características claves de EIGRP:

- Convergencia rápida.

- Utilización reducida del ancho de bando.
- Soporte para múltiples protocolos de capa de red.
- Posibilidades avanzadas de vector-distancia.
- 100% sin bucles.
- Configuración sencilla.
- Actualizaciones incrementales.
- Soporte para VLSM, redes no contiguas.
- Compatibilidad con IGRP.

7.4 VENTAJAS DE EIGRP

EIGRP ofrece muchas ventajas con respecto a los protocolos de ruteo por vector-distancia tradicionales. Una de las ventajas más importantes está en el área del uso del ancho de banda. Con EIGRP, el tráfico operativo es principalmente multidifusión en vez de difusión. Como resultado de ello, las estaciones finales no se ven afectadas por las actualizaciones o consultas de ruteo. EIGRP utiliza el algoritmo IGRP para el cálculo de la métrica, aunque el valor está representado en un formato de 32 bits.

La métrica EIGRP es la métrica IGRP multiplicada por 256. Una de las ventajas significativas de EIGRP consiste en el soporte que da el equilibrio de la carga de métrica desigual.[62]

[62] Permite a los administradores distribuir mejor el flujo del tráfico en sus redes.

Algunas de las características operativas EIGRP se toman de los protocolos del estado de enlace. Por ejemplo, EIGRP permite a los administradores crear rutas de resumen en la posición de cualquier bit en la red, en vez del enfoque tradicional de que los vectores de distancia lleven a cabo resumen de clases en los límites de los principales números de red. EIGRP también soporta la redistribución de ruta de otros protocolos de ruteo.

Al igual que ocurre en todos los protocolos de ruteo TCP/IP, EIGRP se apoya en paquetes IP para dar información de ruteo. El proceso de ruteo EIGRP es una función de la capa de transporte del modelo OSI. Los paquetes IP que llevan información EIGRP utilizan el número de protocolo 88 en sus cabeceras IP. La figura 21, muestra el formato de un paquete IP y los valores que se utilizan para designar el contenido *payload* (carga útil*)* del paquete.[63]

[63] Consultado en http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm

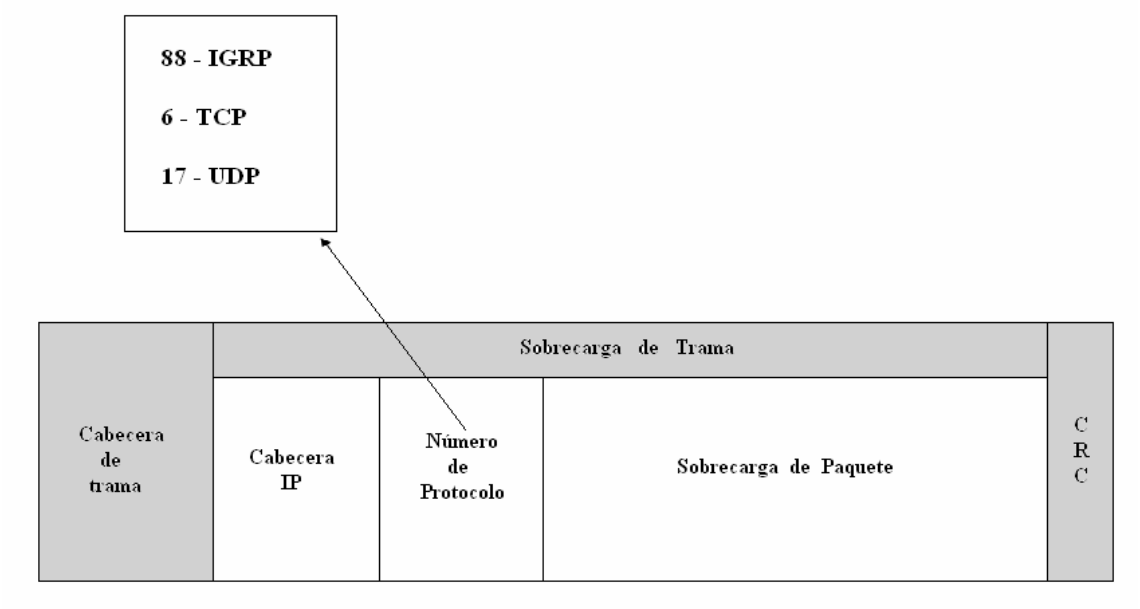


Figura 21. Formato de un paquete IP

EIGRP fue diseñado para funcionar tanto en entornos LAN como WAN. En Topologías multiacceso, como Ethernet y Token Ring, las relaciones de vecindad se forman y mantienen por medio de la multidifusión fiable. EIGRP soporta todas las tecnologías WAN: los enlaces dedicados, los enlaces punto a punto y la topología de multiacceso sin difusión (NBMA).

EIGRP soporta tanto el direccionamiento IP no jerárquico como el no jerárquico. EIGRP también soporta VLSM, con lo que se promueve una asignación eficaz de las direcciones IP. Las direcciones secundarias pueden ser aplicadas a las interfaces con el fin de resolver temas de direccionamiento determinados, aunque todo el tráfico de la estructura de ruteo se genera a través de la dirección de interfaz principal.

Por defecto, EIGRP lleva a cabo el resumen de ruta en los límites de redes principales, como se ve en la figura 22. Además, los

administradores pueden configurar el resumen manual en límites de bit arbitrarios con el fin de reducir el tamaño de la tabla de ruteo. EIGRP soporta la creación de superredes o bloques agregados de direcciones (redes).

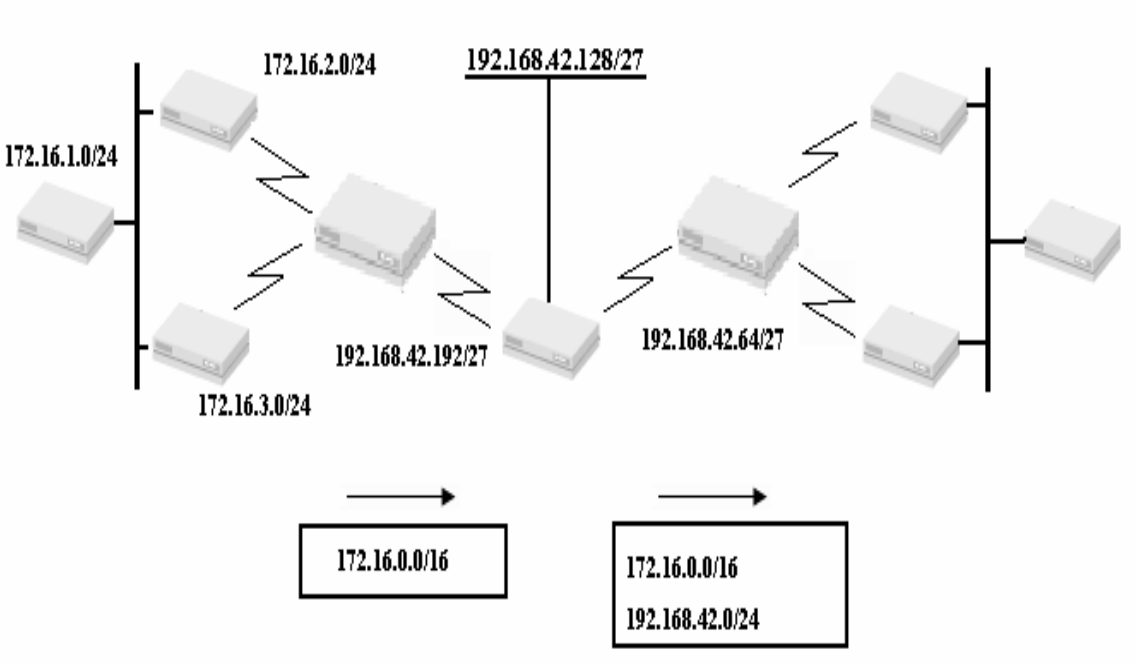


Figura 22.

7.5 PAQUETES EIGRP

EIGRP utiliza estos cinco tipos de paquetes:

- **Hello:** Los paquetes hello se utilizan para el descubrimiento de redes. Son enviados como multidifusión y transportan un número de reconocimiento 0.

- **Actualización:** Las actualizaciones se envían para comunicar las rutas que ha utilizado un determinado ruteador para converger. Estas actualizaciones se envían como multidifusión cuando se descubre una nueva ruta y cuando se completa la convergencia (cuando la ruta se vuelve pasiva). Para sincronizar las tablas de topología, se envían actualizaciones como unidifusión a los vecinos durante la secuencia de inicio de EIGRP. Las actualizaciones se envían de modo fiable.
- **Consultas:** Cuando un ruteador está llevando a cabo el cálculo de ruta y no puede encontrar un sucesor factible, envía un paquete de consulta a sus vecinos, preguntando si tienen un sucesor factible al destino. Las consultas son siempre multidifusión y se envían fiablemente.
- **Respuestas:** Un paquete de respuesta se envía como respuesta a un paquete de consulta. Las respuestas son unidifusión con respecto al origen de la consulta y se envían fiablemente.
- **ACK:** Los ACK se utilizan para confirmar actualizaciones, consultas y respuestas. Los ACK son paquetes hello enviados como multidifusión y contienen un número de acuse de recibo distinto de cero.[64]

[64] Consultado en http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm

8. (PROTOCOLO DE PUERTA DE ENLACE DE FRONTERA) BGP

BGP es un protocolo dedicado a la tarea de determinar la trayectoria en las redes actuales.

BGP desempeña el ruteo entre dominios en las redes que utilizan TCP/IP, lo que significa que lleva a cabo el ruteo entre múltiples AS, e intercambia ruteo e información alcanzable con otros sistemas BGP.

BGP fue desarrollado para que reemplazara a su predecesor, el ahora obsoleto EGP, como el protocolo estándar de ruteo de puerta de enlace exterior utilizado en la red global de Internet.

La figura 23, muestra ruteadores principales que utilizan el BGP para rutear tráfico entre sistemas autónomos (AS).

BGP se especifica en varias RFCs[65]:

- RFC 1771 - describe el BGP4, la versión actual de BGP
- RFC 1654 – describe la primera especificación de BGP4
- RFC 1105, RFC 1163 y RFC 1267 – describe las versiones del BGP anteriores al BGP4

[65] Solicitudes de comentarios.

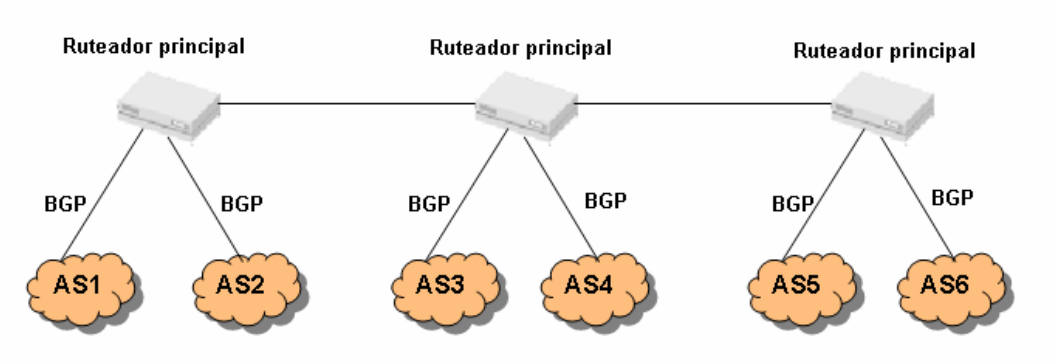


Figura 23. Los ruteadores principales pueden utilizar BGP para rutear tráfico entre AS.

8.1 OPERACIÓN DE BGP

BGP realiza tres tipos de ruteo:

- *Ruteo de sistemas interautónomos*
- *Ruteo de sistemas intraautónomos*
- *Ruteo de sistemas autónomos de paso*

8.1.1 RUTEO DE SISTEMAS INTERAUTÓNOMOS

Se presenta entre dos o más ruteadores BGP en AS diferentes. Los ruteadores equivalentes en estos sistemas utilizan BGP para mantener una vista consistente de la topología de la red. Los BGP vecinos que se comunican entre AS deben residir en la misma red física.[66] Las red Internet es ejemplo de una entidad que utiliza este tipo de ruteo ya que está compuesta por AS. Muchos de estos AS representan a las diferentes

[66] Información obtenida de www.cisco.com/warp/public459/bgp-toc.html

instituciones, corporaciones, y entidades que forman Internet. El BGP se suele utilizar para determinar la trayectoria que proporciones el ruteo óptimo en Internet.

8.1.2 RUTEO DE SISTEMAS INTRAAUTONOMOS

Se presenta entre dos o más ruteadores BGP localizados en el mismo AS. Los ruteadores equivalentes dentro del mismo AS utilizan el BGP para conservar una vista consistente de la topología del sistema. El BGP también se utiliza para determinar qué ruteador servirá como punto de conexión para los AS externos específicos. Una organización, como la una universidad, podría hacer uso del protocolo BGP para ofrecer el ruteo óptimo dentro de su propio AS. El protocolo BGP puede proporcionar servicios de ruteo de sistemas inter e intraautónomos.

8.1.3 RUTEO DE SISTEMAS AUTÓNOMOS DE PASO

Se presenta entre dos o más ruteadores equivalentes BGP que intercambian tráfico a través de un AS que no corre el BGP. En un ambiente de AS de paso, el tráfico BGP no se origina dentro del AS en cuestión y no está destinado a un nodo en el AS. el BGP debe interactuar con cualquier protocolo de ruteo de sistema interautónomo que se esté utilizando para transportar de manera exitosa el tráfico BGP a través de ese AS. la figura 24, muestra un ambiente de AS de paso.[67]

[67] Información obtenida de www.cisco.com/warp/public459/bgp-toc.html

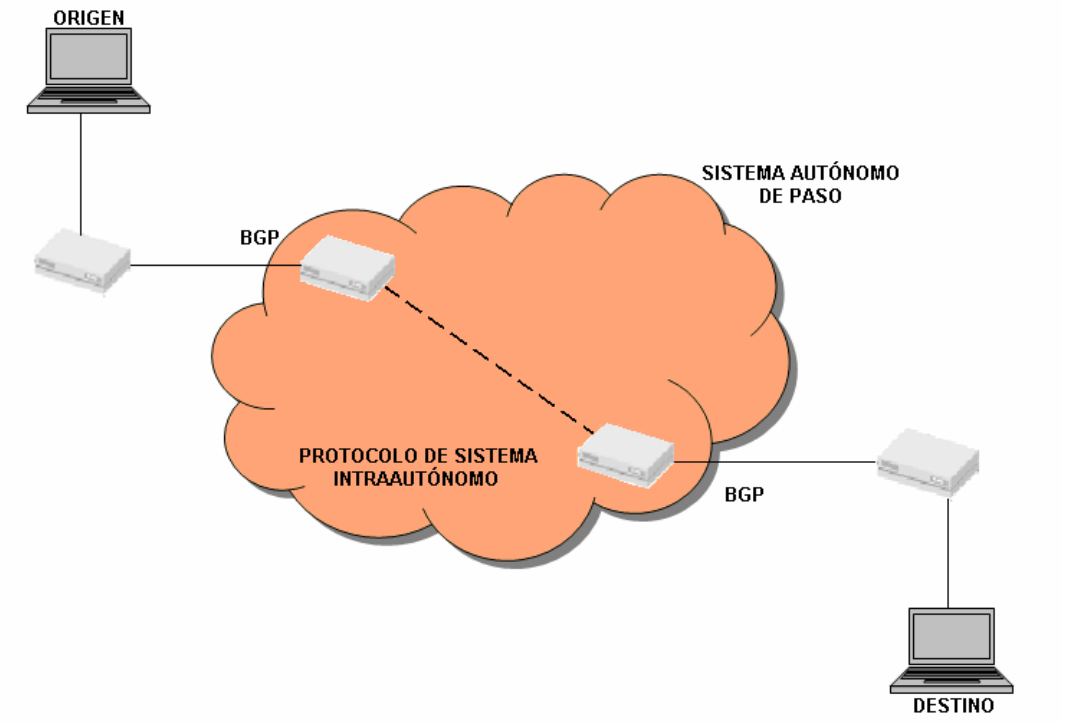


Figura 24. En el ruteo de AS de paso, el BGP se conecta con otro protocolo de ruteo de sistema intraautónomo.

8.2 RUTEO BGP

Igual que con cualquier protocolo de ruteo, el protocolo BGP lleva tablas de ruteo, transmite actualizaciones de ruteo y se basa en medidas para tomar las decisiones de ruteo.

La función principal de un sistema BGP es intercambiar información respecto al alcance de la red, incluyendo información sobre las listas de las trayectorias de AS con otros sistemas BGP. Esta información se puede utilizar para construir una gráfica de la conectividad de los AS de la cual se pueden retirar los ciclos de ruteo y con la que se pueden aplicar las decisiones en cuanto a las medidas que se tomarán a nivel de AS.

Cada uno de los ruteadores BGP lleva una tabla de ruteo que enlista todas las trayectorias factibles a través de una red particular. Sin embargo, el ruteador no actualiza la tabla de ruteo. En vez de ello, la información de ruteo que reciben los ruteadores equivalentes se conserva hasta que se recibe una actualización de incremento.

Los dispositivos BGP intercambian información de ruteo en un intercambio inicial de datos y después con actualizaciones de incremento. Cuando un ruteador se conecta por primera vez a la red, los ruteadores BGP intercambian todas sus tablas de ruteo BGP. De manera similar, cuando se modifica la tabla de ruteo, los ruteadores envían la porción de su tabla de ruteo que se ha modificado. Los ruteadores BGP no envían, de manera regular, actualizaciones de ruteo programado, y las actualizaciones de ruteo BGP anuncian solamente la trayectoria óptima hacia una red.

8.3 MÉTRICA BGP

El BGP utiliza una sola métrica de ruteo para determinar la mejor trayectoria hacia una determinada red. Esta métrica consta de un número arbitrario de unidades que especifica el grado de preferencia de un enlace particular. [68]

[68] Información obtenida de www.cisco.com/warp/public459/bgp-toc.html

La medida BGP típicamente se le asigna a cada enlace a través del administrador de la red.

El valor asignado a un enlace puede basarse en cualquier criterio, entre ellos, la cantidad de AS por los que pasan la trayectoria, la estabilidad, la velocidad, el retardo y el costo.

8.4 CUANDO UTILIZAR BGP

El uso de BGP en un AS es muy apropiado cuando se comprenden bien los efectos de BGP y se da al menos una de estas condiciones:

- Que el AS permita que los paquetes transiten por el para llegar a otros AS (Ejemplo: Proveedor de Servicios)
- Que el AS posea múltiples conexiones con otros AS
- Que el flujo del tráfico que entra y sale del AS está manipulado.

Una decisión sobre normas que deba diferenciar entre el tráfico de un AS y su ISP implica que el AS tiene que conectar su ISP con BGP, en lugar de conectarla con una ruta estática.[69]

BGP fue diseñado para permitir a los ISP comunicarse e intercambiar paquetes. Estos ISP poseen múltiples conexiones entre sí y poseen acuerdos para intercambiar actualizaciones.

[69] Para profundizar, consultar en: tutorial de ruteo con BGP.pdf

Si BGP no es filtrado o controlado correctamente, tiene el potencial de permitir que un AS exterior afecte sus decisiones de ruteo.

8.5 CUANDO NO UTILIZAR BGP

En esta sección mostraremos cuando BGP no es apropiado para ser utilizado en una red, aborda el uso de las alternativa, las rutas estáticas.

BGP no siempre es la solución apropiada para interconectar AS. por ejemplo, si hay una sola ruta, lo adecuado sería una ruta estática.[70] El uso de BGP no nos conduciría a nada, excepto al uso de recursos y memorias de la CPU del ruteador. Si las normas que se implementan en el AS del ISP, no será necesario (ni deseable) configurar BGP en ese AS. Sólo sería necesario cuando las normas locales difieran de las normas del ISP.[71]

No utilice BGP si se da una o más de las siguientes condiciones:

- Que haya una sola conexión con Internet o con otro AS.
- Que no se hayan tenido en cuenta las normas de ruteo ni la selección de ruta
- Que haya una falla de memoria o energía en el procesador en enrutadores que manejan actualizaciones BGP constantemente.

[70] Esta ruta estática es llamada por otros autores como ruta predeterminada
[71] Para profundizar, consultar en: tutorial de ruteo con BGP.pdf

- Que se entienda limitadamente el filtrado de ruta y el proceso de selección de ruta BGP
- Que haya poco anchoa de banda entre dos AS.

En estos casos anteriores, utilice rutas estáticas.

8.6 BGP versión 4

Los principales cambios se aplican al soporte de *"supernetting"* o *CIDR("Classless Inter-Domain Routing")*. En particular, BGP-4 soporta prefijos IP y agregación de rutas. Debido a que CIDR es radicalmente distinto de la arquitectura de ruteo normal de Internet, BGP-4 es incompatible con BGP-3. Sin embargo, BGP define un mecanismo para que dos BGP negocien una versión que ambos entiendan, utilizando el mensaje OPEN. Por lo tanto, es posible implementar BGPS "bilingües" que permiten la interoperatividad entre BGP-3 y BGP-4.[72]

8.7 TIPOS DE MENSAJES EN BGP

En el BGP4, se especifican cuatro tipos de mensajes BGP:

- Mensaje abierto
- Mensaje de actualización
- Mensaje de notificación
- Mensaje de sobrevivencia

8.7.1 MENSAJE ABIERTO

[72] Consultado en http://www.cisco.com/en/US/tech/tk365/tk352/tsd_technology_support_sub-protocol_home.html

Este mensaje abre una sesión de comunicación BGP entre equivalentes y es el primer mensaje enviado por cada lado una vez establecida una conexión del protocolo de transporte. Los mensajes abiertos se confirman a través de un mensaje de sobrevivencia enviado por el dispositivo equivalente y deben ser confirmados antes de que se pueda intercambiar las señales de actualización, notificación y sobrevivencia.

8.7.2 MENSAJE DE ACTUALIZACIÓN

Este mensaje permite que los ruteadores construyan una ruta consistente de la topología de la red. Se envían actualizaciones por medio del TCP para asegurar una entrega confiable. Los mensajes de actualización pueden retirar una o más rutas factibles de la tabla de ruteo y pueden, al mismo tiempo, anunciar una ruta mientras se deshacen de otras.[73]

8.7.3 MENSAJE DE NOTIFICACIÓN

Este mensaje se envía cuando se detecta una condición de error. Las notificaciones se utilizan para cerrar una sesión activa e informar a cualquier ruteador conectado el porque se está cerrando la sesión.

8.7.4 MENSAJE DE SOBREVIVENCIA

[73] Consultado en : Ford, Merilee. Lew, H. Kim. Spanier Steve. Stevenson Tim. CISCO SYSTEMS.

Este mensaje notifica a equivalentes BGP que el dispositivo se mantiene activo. Las señales de sobrevivencia son enviadas con la frecuencia necesaria para evitar que las sesiones expiren.

8.8 FORMATO DE LOS MENSAJES BGP

8.8.1 FORMATO DEL ENCABEZADO

Todos los tipos de mensaje BGP utilizan el encabezado del paquete básico.

Los mensajes abierto, de actualización y notificación tienen más campos, pero los mensajes de sobrevivencia utilizan solo el encabezado de paquete básico. La figura 25 muestra los campos que se utilizan en el encabezado BGP.

8.8.2 CAMPOS DEL ENCABEZADO DE PAQUETE EN BGP

Cada paquete BGP consta de un encabezado cuya función principal es identificar la función del paquete en cuestión.

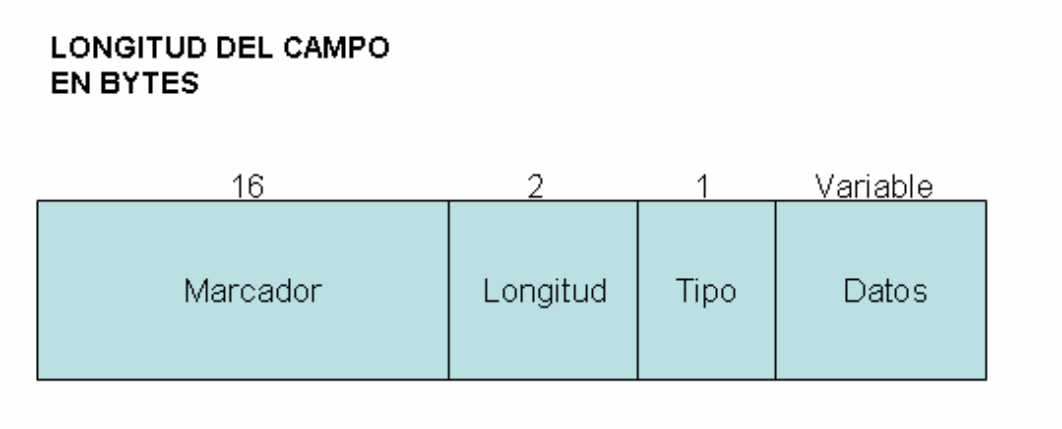


Figura 25. El encabezado del paquete BGP consta de cuatro campos.

- *Marcador:* Consta de un valor de autentificación que puede predecir el receptor del mensaje.
- *Longitud:* Indica la longitud total del mensaje en bytes.
- *Tipo:* Especifica el tipo de mensaje.
- *Datos:* Contiene información sobre las capas superiores en este campo opcional.

8.8.3 FORMATO DEL MENSAJE ABIERTO

Los mensajes abiertos están compuestos por un encabezado BGP y campos adicionales, como se muestra en la figura 26.[74]

[74] Consultado en : Ford, Merilee. Lew, H. Kim. Spanier Steve. Stevenson Tim. CISCO SYSTEMS.

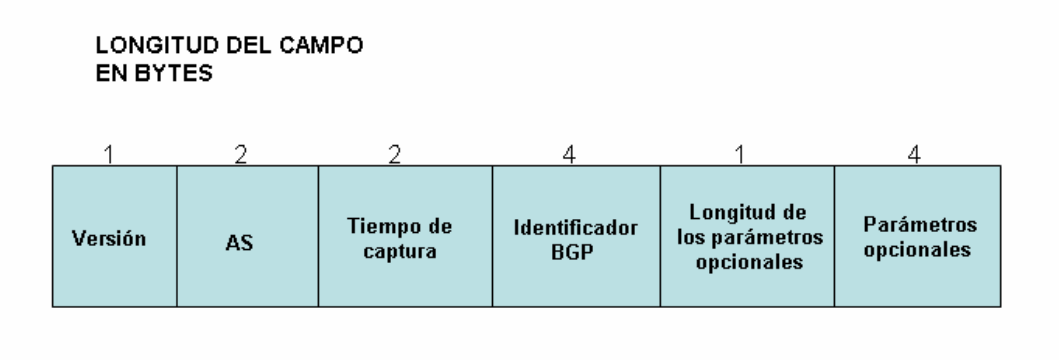


Figura 26. Mensaje abierto BGP consta de seis campos.

- *Versión:* Proporciona el número de versión de BGP para que el receptor pueda determinar si está corriendo la misma versión que el emisor.
- *Sistema Autónomo (AS):* Proporciona el número de AS del emisor.
- *Tiempo de espera:* Indica el número máximo de segundos que pueden transcurrir sin recibir un mensaje, antes de considerar que el transmisor no está funcionando.
- *Identificador de BGP:* Proporciona el identificador BGP del emisor,[75] que se determina en el momento del inicio y es idéntico para todas las interfases locales y todos los BGP equivalentes
- *Longitud de los parámetros opcionales:* Indica la longitud del campo de parámetros opcionales[76].
- *Parámetros opcionales:* consta de una lista de parámetros opcionales (si existe). Actualmente, sólo un tipo de parámetro opcional está definido: la información de autentificación

[75] Proporciona una dirección IP
[76] si están presente

La información de autentificación consta de los dos campos siguientes:

- *Código de autentificación:* Indica el tipo de autenticación que se está utilizando.
- *Datos de autentificación:* Contiene datos que utiliza el mecanismo de autentificación [77]

8.8.4 FORMATO DEL MENSAJE DE ACTUALIZACIÓN

Los mensajes de actualización de BGP constan de un encabezado de BGP y otros campos. La figura 27, muestra los campos adicionales que se utilizan en los mensajes de actualización de BGP.

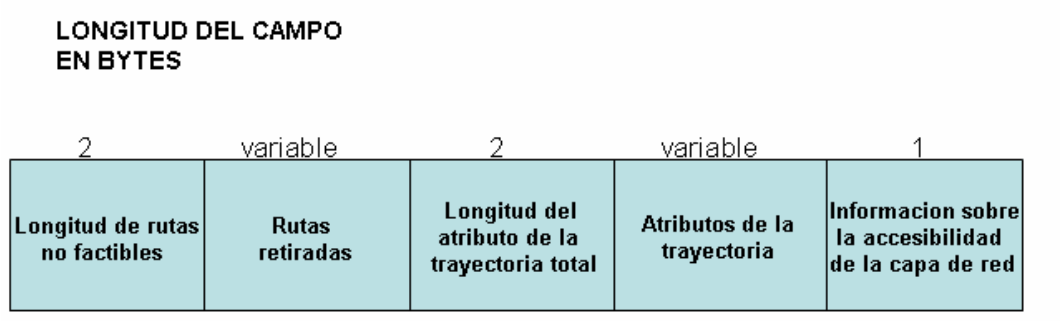


Figura 27. Mensaje de actualización de BGP consta de cinco campos.

- *Longitud de rutas no factibles:* Indica la longitud total del campo de rutas retiradas, o bien que el campo no está presente.
- *Rutas retiradas:* Consta de una lista de prefijos de las direcciones IP para las rutas que se están retirando de servicio.

[77] Si se llegara a utilizar.

- *Longitud total de atributos de la trayectoria:* Indica la longitud total del campo de atributos de la trayectoria o que el campo no está.
- *Atributos de la trayectoria:* Describe las características de la trayectoria anunciada. A continuación mencionaremos los atributos posibles para una trayectoria:
    1. *Origen*
    2. *Trayectoria AS*
    3. *Salto siguiente*
    4. *Mult Exit Disc*
    5. *Preferencia local*
    6. *Agregado atómico*
    7. *Agregador*
- *Información sobre el alcance de la capa de red:* Consta de una lista de prefijos de direcciones IP para las rutas anunciadas.

9. CASOS DE ESTUDIO

Para mayor comprensión de estos casos de estudio, es necesario que tratemos algunos temas antes de observarlos.

9.1 REDISTRIBUCIÓN

Cuando se presenta cualquiera de las situaciones anteriores, los ruteadores permiten a las internetworks que utilizan distintos protocolos de ruteo (a las que se denomina sistemas autónomos) intercambiar la información de ruteo a través de una operación llamada “redistribución de rutas”. La redistribución se define como la capacidad que tienen los ruteadores fronterizos de conectar distintos sistemas autónomos con el fin de intercambiar y publicar información de ruteo recibida de uno a dos o más sistemas autónomos.

En cada AS, los ruteadores internos conocen completamente su red. El ruteador que interconecta AS se denomina ***ruteador fronterizo***.

En la figura 28, el AS 200 está ejecutando el protocolo (IGRP), mientras que el AS 300 está ejecutando el protocolo (EIGRP). Los ruteadores internos de cada AS conocen sus redes completamente.[78]

[78] Para profundización de redistribución consultar **Paquet, Catherine**. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables.

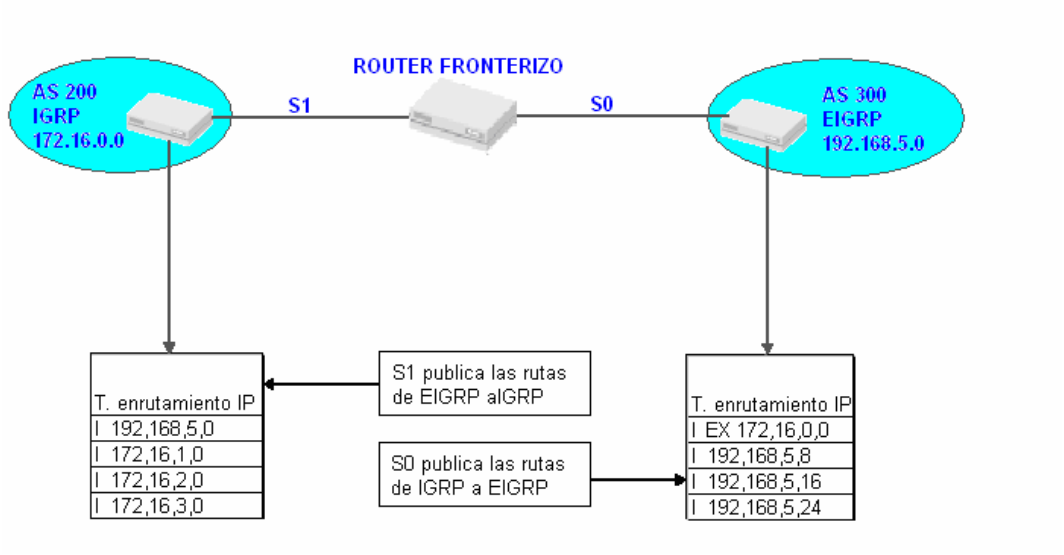


Figura 28. Redistribución entre un AS IGRP y EIGRP.

El ruteador A es el fronterizo. Este ruteador tiene los procesos IGRP y EIGRP activados, y es el encargado de publicar las rutas conocidas de un AS al otro.

El ruteador A conoce la red 192.168.5.0 del ruteador B a través del protocolo EIGRP que se ejecuta en su interfaz S0. Pasa (redistribuye) esa información al ruteador C en su interfaz S1 a través de IGRP. La información de ruteo también se pasa (redistribuye) de la otra forma, de IGRP a EIGRP.

La tabla de ruteo del ruteador B muestra que ha conocido la red 172.16.0.0 a través de EIGRP (tal como indica la “D” de la tabla de ruteo) y que la ruta es externa a este AS (tal como indica la “EX” de la tabla de ruteo). La tabla de ruteo del ruteador C muestra que ha conocido la red 198.168.5.0 a través de IGRP (como indica la “I” de la tabla de ruteo).

Observe que, a diferencia de EIGRP, no hay indicación de IGRP de si una ruta es externa o interna al AS.

9.2 REDISTRIBUCIÓN ENTRE MÚLTIPLES PROTOCOLOS DE RUTEO

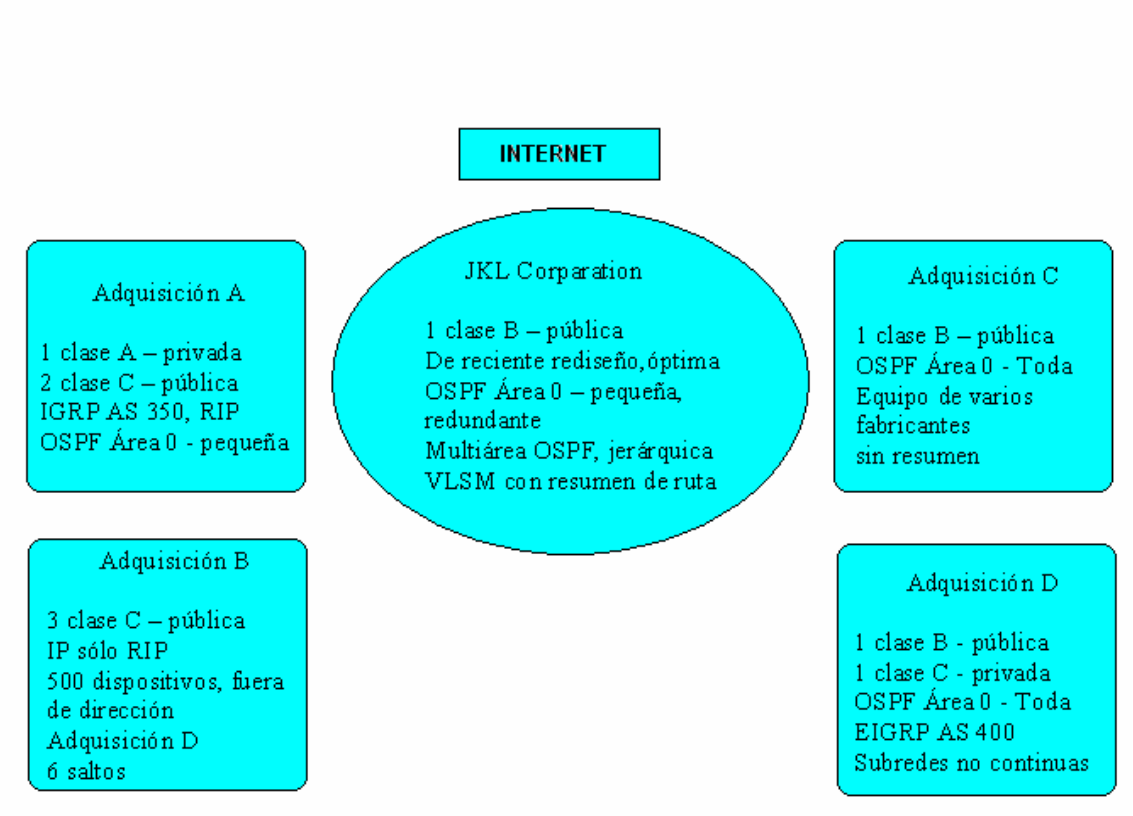
Algunas veces será necesario utilizar mas de un protocolo de ruteo, a continuación veremos las posibles razones por las que pueden ser necesarios múltiples protocolos.

- Está migrando de un protocolo de gateway interior (IGP) a un nuevo (IGP). Puede haber múltiples límites de redistribución hasta que el nuevo protocolo haya desplazado por completo al viejo protocolo.
- Desea usar otro protocolo, pero necesita mantener el antiguo, debido a las necesidades de los sistemas *host.*
- Es posible que los distintos departamentos no quieran actualizar sus ruteadores, o que no quieran implementar unas normas de filtrado lo suficientemente estrictas. En estos casos puede protegerse a sí mismo cerrando el otro protocolo de ruteo de uno de sus ruteadores.
- Si tiene un entorno de fabricante con ruteador mixto, un ejemplo sería: se puede usar un protocolo específico CISCO en la parte CISCO de la red, para luego usar un protocolo común para comunicarse con dispositivos que no sean CISCO.[79]

[79] Obtenido de **Paquet, Catherine**. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables.

9.3 ADQUISICIONES DE JKL CORPORATION

En estos casos de estudio utilizamos casos prácticos de **JKL Corporation,** como se observa en la figura mostrada a continuación, para discutir los distintos aspectos del ruteo. Las secciones de estos casos se utilizan para repasar los conceptos, para discutir los temas vitales que giran en torno al funcionamiento de las redes, y para dar un enfoque de los ejercicios de configuración. [80]



[80] Explicación obtenida de **Paquet, Catherine**. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables.

Figura 29. Clases de Adquisiciones de JKL.

El ejemplo JKL Corporation se utiliza en los casos de estudio de este documento.

En los casos de estudio, JKL es una empresa que va a realizar cuatro posibles adquisiciones (A, B, C y D).

En cada caso de estudio se ofrecen sugerencias, soluciones y respuestas en base al problema planteado.

9.4 CASO DE ESTUDIO “OSPF EN UNA SOLA AREA”

Los protocolos de ruteo por estado de enlace, como OSPF, suelen desplegarse en redes medianas y grandes. La implementación de OSPF suele empezar con la creación del área 0, que es el núcleo de la red. En la figura mostrada a continuación, muestra la adquisición C de JKL, se seleccionó OSPF, ya que se están usando distintos equipos de fabricantes y se requiere un protocolo de ruteo no propietario. Hay menos de 20 ruteadores en la red, y todos ellos forman parte del núcleo del área 0.[81]

Mientras examinamos la figura, analizaremos lo siguiente:

- Consideraciones relativas a la topología.
- Limitaciones en la métrica
- Trafico de actualización del ruteo
- Tiempo de convergencia
- Facilidad de configuración y administración

[81] Caso de estudio obtenido de **Paquet, Catherine**. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables.

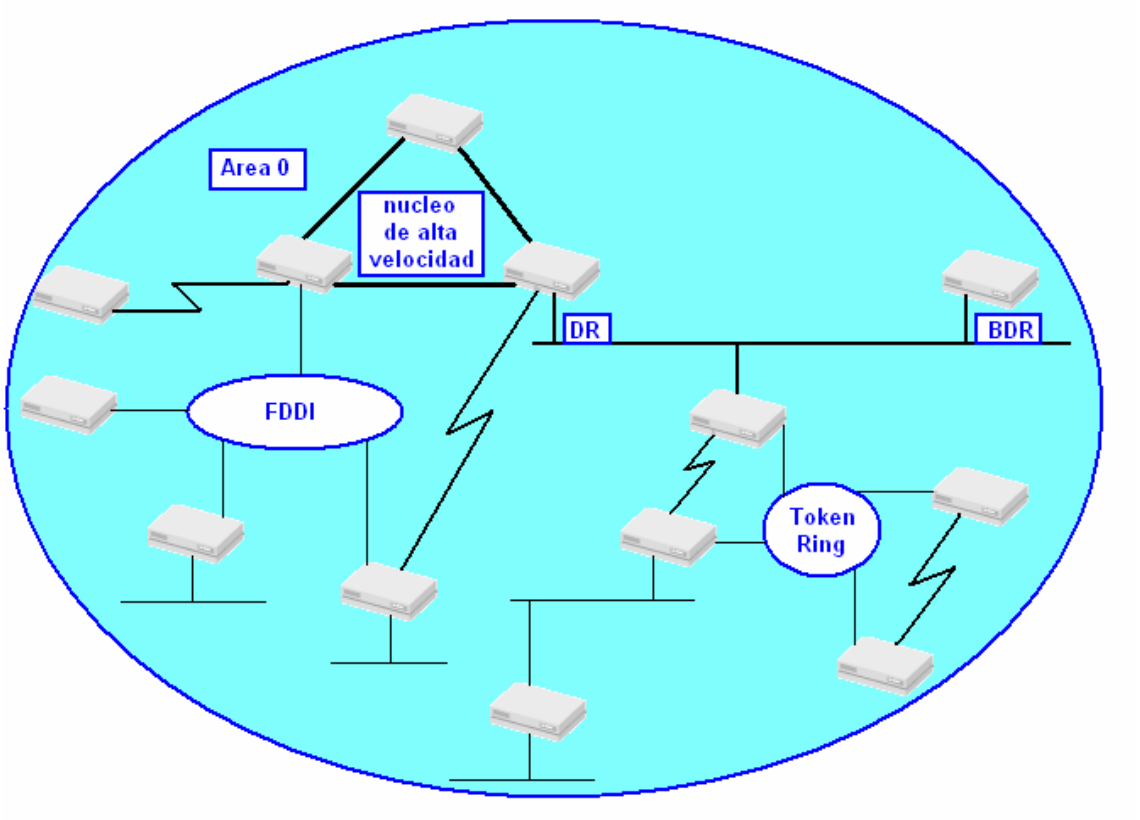


Figura 30. OSPF en una sola área

SOLUCIÓN:

La red de adquisición C ha existido durante unos cuantos años, y la infraestructura refleja las distintas tecnologías que fueron seleccionadas, ya que ofrecían el ancho de banda más alto disponible en el momento de su creación. La administración de la adquisición C siempre tuvo la velocidad como preocupación principal y, como consecuencia de ello, seleccionó un protocolo de ruteo por estado de enlace (OSPF), debido a su rápida convergencia. En un intento de controlar los costos, al tiempo

que se desplegaba la tecnología más actual, la administración adquirió equipos de distintos fabricantes.

El uso de equipos de varios fabricantes y enlaces de alta velocidad pueden requerir ajuste de los costos de la interfaz OSPF.

El crecimiento de la red de C se ha realizado de un modo *ad hoc,* en vez de realizarlo con diseño. Este crecimiento aleatorio ha originado que las direcciones de subred se distribuyan arbitrariamente por la red. Por tanto, debido al espacio de direcciones de subred no continuo de esta red, el resumen de ruta podría ser imposible. Además, dado que todos los ruteadores se encuentran en el área 0 (y por tanto, no hay jerarquía), no existen ruteadores de límite de área (ABR) en los que configurar el resumen.

La falta de ruta implica que las tablas de ruteo son mas grandes de lo necesario.

El crecimiento aleatorio también ha excluido toda idea de crear una topología jerárquica con lo ruteadores desplegados en base a la funcionalidad.

El fallo de cualquier enlace crea una interrupción del tráfico en todas las partes de la red y podría consumir una parte importante del ancho de banda. Los intentos de aumentar la fiabilidad creando rutas redundantes por la red solo han sido satisfactorios en parte. La velocidad de las rutas alternativas es muy distinta a la velocidad de los enlaces principales, y

esto significa que las publicaciones del estado de enlace pueden no funcionar.

Además, la administración de esta red podría ser más difícil de manejar que lo normal, debido a su entorno de varios fabricantes y a la falta de jerarquía.

9.5 CASO DE ESTUDIO "REDISTRIBUCIÓN (OSPF, IGRP Y RIP)"

Luego de observar la información introductoria con referencias a los casos de estudio.

En este caso de estudio examinaremos cómo la adquisición A de JKL va a implementar sus protocolos IGRP, RIP y OSPF. Posee dos direcciones públicas de clace C y utiliza una dirección privada de clase A. como se ve en la figura mostrada a continuación, cada uno de los tres dominios de protocolo está conectado con los otros dos.[82]

Mientras observamos la figura, analizaremos lo siguiente:

- Las limitaciones en el tamaño de un dominio de ruteo.
- El uso de una distancia administrativa como mecanismo de aprendizaje
- Las posibilidades de que haya rutas subóptimas en la tabla de ruteo
- La protección frente a bucles de información, en especial aquellos causados por los cambios en la topología.
- El requisito para la métrica de generación apropiada a la hora de pasar las rutas entre los distintos protocolos.

[82] Caso de estudio obtenido de **Paquet, Catherine**. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables.

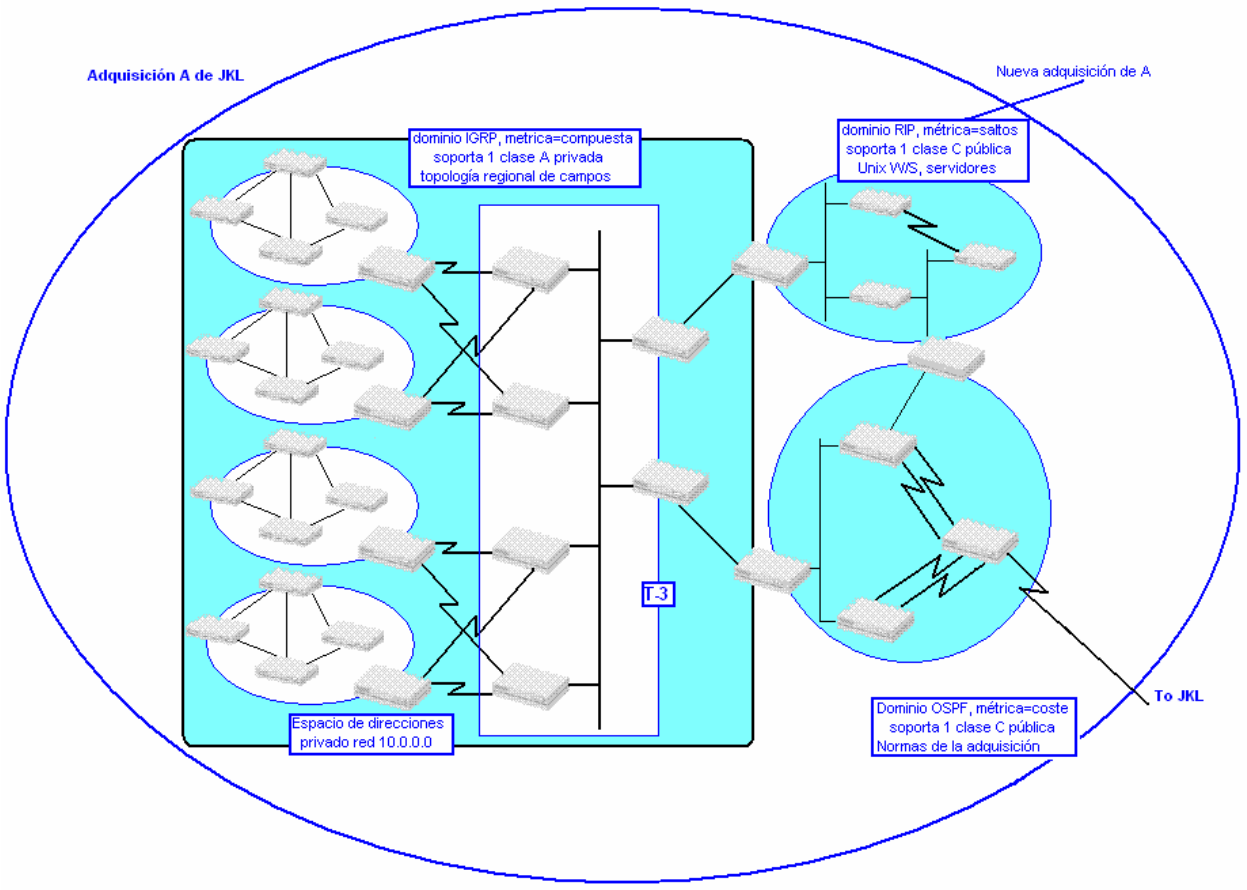


Figura 31. Redistribución (OSPF, RIP y IGRP)

SOLUCIÓN:

La red de la adquisición A fue originariamente una implementación RIP, hasta que creció demasiado. Se seleccionó IGRP y el direccionamiento privado para manipular la parte más grande de la red, ya que IGRP es una red de campus regional jerárquica con resumen de ruta en los ruteadores D y G.

El dominio RIP de la parte superior derecha de la figura representa una concentración de estaciones de trabajo y servidores UNIX y que no se encuentran bajo el control administrativo de A. el espacio de direcciones

de clase C del dominio RIP se resume en un límite con clase en los ruteadores G y H.

Originariamente, el dominio OSPF era un dominio RIP, pero ha sido convertido a OSPF antes de la consolidación de la red empresarial de JKL. La conexión con Internet se realiza actualmente a través del ruteadores A, aunque éste enlaza finalmente toda la red con JKL.

Las distancias administrativas de IGRP, OSPF y RIP son, respectivamente, 100, 110 y 120.

Si se produjera una redistribución en ambos sentidos de cada dominio en los ruteadores D, G y H, se podrían propagar rutas subóptimas, ya que la distancia administrativa de IGRP es menor. En una topología de bucles potencial, como la que se muestra en la figura, hay que tener cuidado a la hora de aplicar los filtros de ruta con el fin de evitar la información de rutas conocidas a través de la redistribución. Este tipo de rutas empieza con una métrica de generación especificada por el comando *redistribuye.* Las rutas subóptimas podrían tener una métrica deficiente (que indicara una ruta no deseable), pero siguen siendo las rutas preferidas, ya fueron conocidas por un protocolo de ruteo provisto de una distancia administrativa superior, “existe una diferencia significativa entre el valor de distancia administrativa, que es el factor de preferencia sobre cómo se conocen las rutas, y el valor de la métrica, que es un factor de preferencia que sirve para seleccionar rutas para reenviar el tráfico”.

Las alternativas a la redistribución potencial pueden ser una combinación de rutas estáticas, rutas predeterminadas e instrucciones de interfaz pasiva. En lugar de una redistribución completa en el dominio RIP, piense en el uso de una ruta estática a la red 10.0.0.0, y en rutas predeterminadas en cada ruteador que señalen al dominio OSPF (a través del ruteador H) como punto de salto a Internet.

Algunos puntos que conviene recordar a la hora de considerar la redistribución son las siguientes:

La redistribución es necesaria cuando hay que intercambiar las rutas que tienen estructuras métricas distintas.

La configuración correcta para la redistribución de rutas requiere una instrucción de métrica predeterminada para establecer una métrica de generación.

Las topologías redundantes pueden crear bucles de información que propaguen rutas subóptimas.

El filtrado de ruta es una forma de controlar los bucles de información.

La redistribución completa en ambos sentidos no es la única forma de establecer la conectividad entre dominios de ruteoss distintos.

La distancia administrativa indica la preferencia del ruteador por cómo se conoce una ruta, mientras que el valor de la métrica es una medida de posibilidad de conectar con una ruta.

9.6 CASO DE ESTUDIO “BGP”

En esta aplicación, examinaremos como JKL se conecta a Internet. Como se ve en la figura mostrada a continuación, JKL es el sistema autónomo 65106 y posee dos conexiones ISP, con el sistema autónomo 64573. Como sabe, JKL ejecuta el protocolo primero la ruta libre mas corta (OSPF) como IGP. JKL debe considerar métodos para seleccionar qué ISP va a manejar el grueso de su tráfico de red en los distintos momentos del día.[83]

Mientras examinamos la figura, analizaremos lo siguiente:

- Qué requisitos de topología determinarán qué ruteadores van a ejecutar BGP.
- Si es necesaria la sincronización entre BGP y el IGP.
- Los temas relativos a la redistribución entre un IGP y BGP.
- El método de publicación de ruta para las rutas enviadas y recibidas de Internet
- Facilidad de configuración y administración.

[83] Caso de estudio obtenido de **Paquet, Catherine**. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables.

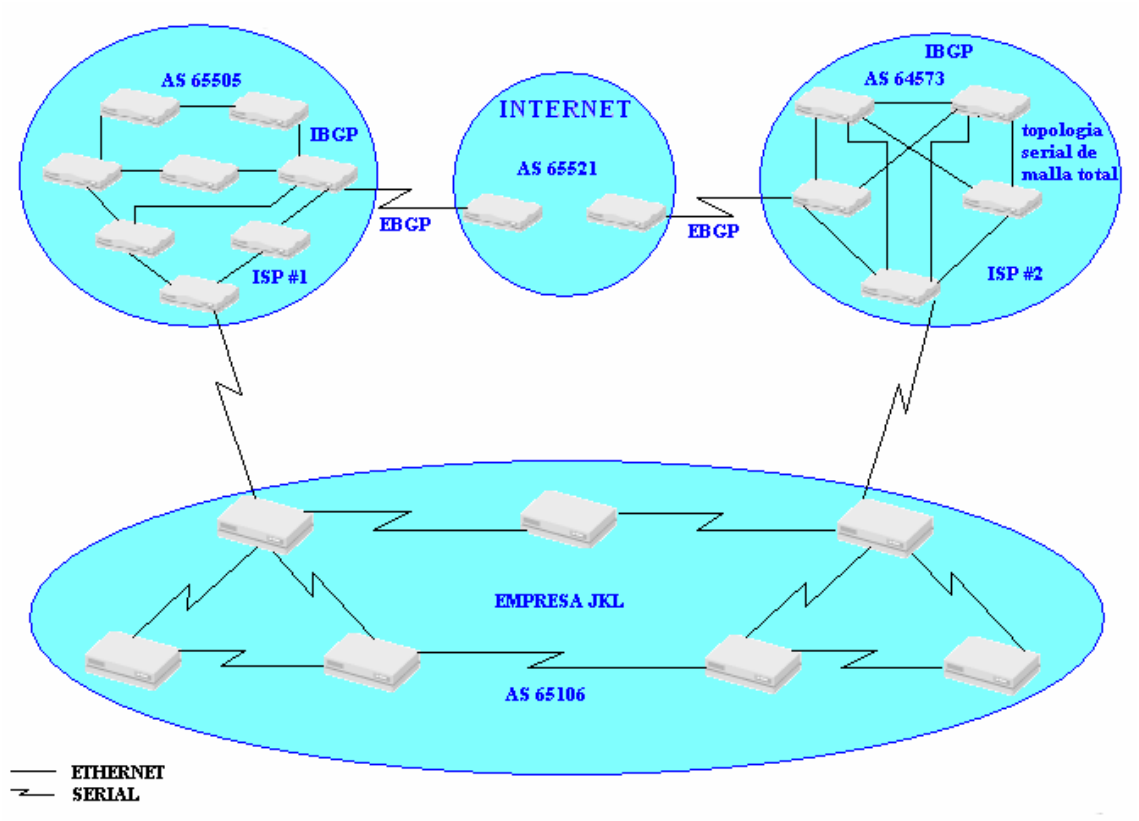


Figura 32. BGP (EBGP y IBGP)

SOLUCION:

JKL necesita una conectividad total a Internet para dirigir el comercio electrónico. Dos ruteadores separados (ubicados en el núcleo de la red corporativa) proporcionan la conectividad física con Internet. Cada uno de los ruteadores mantiene una conexión con un ISP distinto, y esto crea una topología BGP con múltiples conexiones.

Los ruteadores A y B ejecutan BGP. Los ruteadores A y B pertenecen a un sistema autónomo registrado y mantienen una relación EBGP con sus respectivos ISP.

Los ruteadores A y B solo tendrían que tener una relación IBGP entre sí si el sistema autónomo proporcionara una ruta de tránsito a otros sistemas autónomos. Con toda probabilidad éste no es el caso, ya que si así fuera, todos los ruteadores del sistema autónomo de la ruta entre los ruteadores A y B tendría que ejecutar BGP o BGP tendría que ser redistribuido en el sistema autónomo. JKL pidió que solo se proporcionaran las rutas predeterminadas desde ambos ISP.

Los ruteadores A y B han sido configurados con interfaces *loopback* con el fin de dotar de estabilidad al establecimiento de sesiones con ruteadores iguales. Como miembros del núcleo OSPF de JKL, los ruteadores A y B también deben ser configurados para ejecutar un IGP (en este caso, OSPF). El núcleo OSPF utiliza rutas predeterminadas para dirigir el tráfico interno a Internet. La estrategia de usar rutas predeterminadas para el tráfico saliente significa que la información BGP de OSPF no es un requisito para llegar a Internet, el tráfico saliente solo tiene que seguir la ruta ya definida por la ruta predeterminada.

Es importante entender algunos de los temas relacionados con la redistribución entre IGP y BGP. Si los ruteadores A y B estuvieran ejecutando IBGP y las rutas BGP aprendidas por el ruteador A de ISP 1 fueran redistribuidas en el IGP (en este caso OSPF), pasarían a través del

sistema autónomo al ruteador B. si estas rutas (y otras rutas interiores) fueran redistribuidas desde el IGP del ruteador B a BGP, podría haber serios problemas, incluyendo la presencia de mas de 70.000 rutas en la tabla de ruteo y la pérdida de la ruta de sistema autónomo y los demás atributos BGP cuando estas rutas entraran en el IGP.

Los ruteadores A y B publican el sistema autónomo 65106 a ambos ISP, que los procesan y los pasan a otros sistemas autónomos. La ruta que toman los paquetes entrantes para llegar a JKL, dentro de los ISP y otros sistemas autónomos. En la topología que se muestra en la figura, el tráfico de retorno entraría en JKL a través de uno de los ISP, determinado por la longitud de ruta de sistema autónomo, si todos los demás parámetros fueran equivalentes. Establecer el parámetro MED en los ruteadores A y B para tratar de afectar a la ruta de retorno no tendría en este caso efecto alguno. Esto se debe a que los ruteadores están conectados a distintos ISP, y el atributo MED no se pasa con las actualizaciones; sería restablecido a su valor predeterminado de 0 cuando se pasaran las actualizaciones

Algunos de los puntos importantes de este caso práctico son:
Los ruteadores A y B forman una sesión EBGP con sus respectivos ISP.

Si se usan unas normas de ruta predeterminadas en el núcleo JKL para reenviar tráfico a los ISP, la redistribución de ruta entre BGP y OSPF sería innecesaria.

El algoritmo de selección de ruta BGP comprueba varios criterios, entre los que se incluyen los siguientes:

- El peso Cisco más alto
- La preferencia local más alta
- Originado localmente por este *ruteador*
- Ruta de sistema autónomo más corta.
- Código de origen más bajo
- Valor MED más bajo
- EBGP mejor que IBGP.
- Ruta interna más corta en el sistema autónomo para llegar al destino
- Ruta EBGP más antigua.
- ID de ruteador BGP más bajo.
- El comando *network* de BGP funciona de modo distinto que el comando *network* de los IGP.

10. CONCLUSIONES

El avance de las redes de comunicación en general (dispositivos, protocolos y demás elementos de redes), es cada vez mayor y por ello es necesario conocer sus actualizaciones para no quedarnos obsoletos.

Existen muchos protocolos de ruteo pero como todo, son solo pocos los que abarcan gran cantidad de características eficientes para el ruteo.
Los protocolos de ruteo interno IGP son para usos específicos dentro de los sistemas autónomos (AS), al contrario de los protocolos de ruteo externo EGP que son utilizados para intercomunicación de sistemas autónomos. Pero hay protocolos dentro de los IGP, ya mencionados que pueden llegar a intercomunicar sistemas autónomos, y en los EGP también sucede lo mismo pero que pueden llegar a rutear dentro de los sistemas autónomos.

En la actualidad las redes están diseñadas para soportar gran variedad de protocolos de ruteo y sus distintas versiones, en una red puede haber mas de un protocolo de ruteo.
Se puede apreciar en los casos de estudio en una red habían tres protocolos OSPF, RIP y IGRP, y la red estaba funcionando perfectamente.

A medida que transcurre el tiempo los protocolos de ruteo van a seguir siendo mejorados en sus nuevas versiones, o reemplazados por otros protocolos como lo ocurrido con EGP que quedó obsoleto y fue reemplazado por BGP.

10.1 GENERALIDADES

En este recurso se explicó con la mayor claridad posible como tema general los protocolos de ruteo, se trataron temas como los protocolos más importantes y de mayor uso en la actualidad tanto internos como externos, los protocolos como todo lo relacionado con el mundo de la tecnología avanzan muy rápidamente a veces si darnos cuenta.

Estudiantes próximos interesados en profundizar la investigación a cerca de los protocolos de ruteo deberán tener en cuenta que los protocolos explicados en este recurso fueron protocolos actuales y por ende deberán investigar los avances, nuevas versiones existentes y ya implementadas en redes reales, fallas, ventajas y desventajas de las nuevas versiones o nuevos protocolos con los anteriores.

Se puede pensar en la posibilidad de darles a estos protocolos implementaciones en la Universidad de modo que la red de esta se aproveche al máximo. Para esto se tomarán en cuenta los casos de estudio de este medio, que exponen problemas y soluciones reales a estos protocolos.

11. BIBLIOGRAFÍA

11.1 LIBROS

Comer, Douglas. Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura. Tercera edición. De este libro se consultó, *Direccionamiento IP y Ruteo IP*.

Comer, Douglas Interconectividad de Redes con TCP/IP. Diseño e Implementación. Tercera edición. De este libro se consultó, *Protocolo De Información De Ruteo (RIP) y OSPF (Abrir Primero La Ruta Más Corta).*

Doyle, Jeff. DeHaven, Jerrnifer. CISCO SYSTEMS. Routing TCP/IP. Volume II. De este libro se consultó, (*Exterior Gateway Protocol) EGP,* IGRP (Interior Gateway Routing Protocol)

Ford, Merilee. **Lew, H. Kim**. **Spanier Steve**. **Stevenson Tim**. **CISCO SYSTEMS**. Tecnologías de Interconectividad de Redes. De este libro se consultó, (*BORDER GATEWAY PROTOCOL) BGP.*

Gallo, Michael. Hancock, William. Comunicaciones Entre Computadoras y Tecnología de Redes. De este libro se consultó, *Red y Difusión.*

Paquet, Catherine. **Teare, Diane**. **CISCO SYSTEMS**. Creación de Redes Cisco Escalables. De este libro se consultaron todos los "*Casos de Estudio".*

Stallings, William. Comunicación y Redes de Computadores. Séptima edición. De este libro se consultó, *Conceptos de Protocolo.*

11.2 SITIOS WEB

- Tutorial de ruteo en Internet BGP en: tutorial de ruteo con BGP.pdf, en este medio se consultó *CUANDO UTILIZAR BGP y CUANDO NO UTILIZAR BGP*
- Documento Internet Protocolos de Ruteo en: http://www.cisco.com/en/US/tech/tk365/tk352/tsd_technology_support_sub-protocol_home.html, en este medio se consultó *BGP versión 4*
- Documento Internet BGP en: http://www.cisco.com/warp/public/459/bgp-toc.html, en este medio se consultó *BGP versión 4*
- Documento Internet rcf1772 en: http://www.javvin.com/protocol/rfc1772.pdf, en este medio se consultó el *RFC 1772*
- Documento Internet rcf1773 en: http://www.javvin.com/protocol/rfc1773.pdf, en este medio se consultó el *RFC 1773*
- Documento Internet rcf1773 en: http://www.javvin.com/protocol/rfc1774.pdf, en este medio se consultó el *RFC 1774*
- http://www.ietf.org

- Documento Internet Protocolo BGP en: http://www.javvin.com/protocolBGP.html, en este medio se consultó *TIPOS DE MENSAJES EN BGP*
- Documento en Internet 459 BGP en: www_cisco_com-warp-public-459-bgp-toc , en este medio se consultó *CONVERGENCIA RÁPIDA, UTILIZACIÓN REDUCIDA DEL ANCHO DE BANDA, SOPORTE DE CAPA DE MÚLTIPLES REDES, y demás temas relacionados con IGRP.*
- Documento en Internet de Protocolo IGRP en: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm, en este medio se consultó *VENTAJAS DE EIGRP y PAQUETES EIGRP*
- Documento en Internet de Protocolos TCP/IP en: http://ditec.um.es/laso/docs/tut-tcpip/3376c34.html, en este medio se consultó *parte de información de fundamentación*
- Documento en Internet de Tutorial de Redes en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html, en este medio se consultó *PROTOCOLO DE PASARELA INTERIOR (IGP)*
- Documento en Internet Routing en: www.cuyamaca.edu/gainswor/ccna2/Routing_ch7.ppt, en este medio se consultó *temas relacionados con protocolos de ruteo en general.*

12. GLOSARIO

A

Administración de red: Uso de sistemas o acciones para mantener, caracterizar o realizar el diagnóstico de fallas de una red.

Algoritmo: Ver protocolo.

Ancho de banda: Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red. Asimismo, la capacidad de rendimiento medida de un medio o protocolo de red determinado.

B

Backbone: Núcleo estructural de la red, que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

BGP (*protocolo de gateway fronterizo*): Protocolo de ruteo interdominios que reemplaza a EGP. BGP intercambia información de accesibilidad con otros sistemas BGP y se define en RFC 1163.

Bit: Dígito binario utilizado en el sistema numérico binario. Puede ser cero o uno. Ver también byte.

Broadcast: Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

Bucle: Ruta donde los paquetes nunca alcanzan su destino, sino que pasan por ciclos repetidamente a través de una serie constante de nodos de red.

Byte: Serie de dígitos binarios consecutivos que operan como una unidad (por ejemplo, un byte de 8 bits). Ver también bit.

D

Datagrama: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos

Datagrama IP: Unidad fundamental de información transmitida a través de la Internet. Contiene direcciones origen y destino junto con datos y una serie de campos que definen cosas tales como la longitud del datagrama, la suma de verificación del encabezado y señaladores para indicar si el datagrama se puede fragmentar o ha sido fragmentado.

Datos: Datos de protocolo de capa superior.

Dirección: Estructura de datos o convención lógica utilizada para identificar una entidad única, como un proceso o dispositivo de red en particular

E

Enlace: Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor. Se utiliza con mayor frecuencia para referirse a una conexión de WAN. A veces se denomina línea o enlace de transmisión.

Enlace punto a punto: Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde las instalaciones del cliente a través de una red de carrier, como, por ejemplo, la de una compañía telefónica, a una red remota. También denominado enlace dedicado o línea arrendada.

Ruteo: Proceso de descubrimiento de una ruta hacia el host destino. El ruteo es sumamente complejo en grandes redes debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Ruteo del camino más corto: Ruteo que reduce al mínimo la distancia o costo de la ruta a través de una aplicación de un algoritmo.

Ruteo dinámico: Ruteo que se ajusta automáticamente a la topología de la red o a los cambios de tráfico. También denominado ruteo adaptable. Comparar con ruteo estático.

Ruteo estático: Ruta que se ha configurado e introducido explícitamente en la tabla de ruteo Las rutas estáticas tiene prioridad sobre las rutas elegidas por los protocolos de ruteo dinámico. Comparar con ruteo dinámico.

Escalabilidad: Capacidad de una red para aumentar de tamaño sin que sea necesario realizar cambios importantes en el diseño general.

F

Filtro: En general, se refiere a un proceso o dispositivo que rastrea el tráfico de red en busca de determinadas características, por ejemplo, una dirección origen, dirección destino o protocolo y determina si debe enviar o descartar ese tráfico basándose en los criterios establecidos.

G

Gateway: En la comunidad IP, término antiguo que se refiere a un dispositivo de ruteo. Actualmente, el término ruteador se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro. Comparar con ruteador.

H

Host o Anfitrión: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y ruteadores. Ver también nodo.

I

IGRP (*Protocolo de ruteo de gateway interior*): Protocolo desarrollado por Cisco para tratar los problemas asociados con el ruteo en redes heterogéneas de gran envergadura

Interfaz: Conexión entre dos sistemas o dispositivos. 2. En terminología de ruteo, una conexión de red. 3. En telefonía, un límite compartido definido por características de interconexión física comunes, características de señal y significados de las señales intercambiadas. 4. Límite entre capas adyacentes del modelo de referencia OSI

L

LAN (*red de área local*) **:** Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI.

Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas. Comparar con MAN y WAN. Ver también VLAN.

M

Máscara: Ver máscara de dirección y máscara de subred.

Máscara de dirección: Combinación de bits utilizada para describir cuál es la porción de una dirección que se refiere a la red o subred y cuál es la que se refiere al host. A veces se llama simplemente máscara

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Mensaje: Agrupación lógica de información de la capa de aplicación, a menudo compuesta por una cantidad de agrupaciones lógicas de las capas inferiores, por ejemplo, paquetes. Los términos datagrama, trama, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Métrica de ruteo: Método mediante el cual un protocolo de ruteo determina que una ruta es mejor que otra. Esta información se almacena en tablas de ruteo. Las métricas incluyen ancho de banda, costo de la comunicación, retardo, número de saltos, carga, MTU, costo de ruta, y confiabilidad. A menudo denominada simplemente métrica.

N

Networking: Interconexión de estaciones de trabajo, dispositivos periféricos (por ejemplo, impresoras, unidades de disco duro, escáneres y CD-ROM) y otros dispositivos.

Nodo: Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Los nodos pueden ser procesadores, controladores o estaciones de trabajo. Los nodos, que varían en cuanto al ruteo y a otras aptitudes funcionales; pueden estar interconectados mediante enlaces y sirven como puntos de control en la red. La palabra nodo a veces se utiliza de forma genérica para hacer referencia a cualquier entidad que tenga acceso a una red y frecuentemente se utiliza de modo indistinto con la palabra dispositivo.

Número de saltos: Métrica de ruteo utilizada para medir la distancia entre un origen y un destino. RIP utiliza el número de saltos como su métrica exclusiva.

O

OSI (*internetwork de sistemas abiertos*): Programa internacional de estandarización creado por ISO e UIT-T para desarrollar estándares de networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

OSPF (*Primero la ruta libre más corta*): Protocolo de ruteo por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la

comunidad de Internet. Entre las características de OSPF se incluyen el ruteo de menor costo, el ruteo de múltiples rutas, y el balanceo de carga.

P

Paquete: Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

Paquete hello: Paquete multicast utilizado por ruteadores que utilizan ciertos protocolos de ruteo para el descubrimiento y recuperación de vecinos. Los paquetes hello también indican que un cliente se encuentra aún operando y que la red está lista.

R

Red: Agrupación de computadores, impresoras, ruteadores, switches y otros dispositivos que se pueden comunicar entre sí a través de algún medio de transmisión.

Red con productos de varios fabricantes: Red que usa equipamiento de más de un fabricante. Las redes con productos de varios fabricantes

presentan muchos más problemas de compatibilidad que las redes con productos de un solo fabricante. Comparar con red de un único fabricante.

Red de área local: Ver LAN.

Red híbrida: Internetwork de redes compuesta por más de un tipo de tecnología de red, incluyendo LAN y WAN.

Red interna: Red interna a la que tienen acceso los usuarios con acceso a la LAN interna de una organización.

S

Salto: Pasaje de un paquete de datos entre dos nodos de red (por ejemplo, entre dos ruteadores).

Segmentación: Proceso de división de un solo dominio de colisión en dos o más dominios de colisión para reducir las colisiones y la congestión de la red.

T

Tabla de Ruteo: Tabla almacenada en un ruteador o en algún otro dispositivo de internetwork que realiza un seguimiento de las rutas hacia destinos de red específicos y, en algunos casos, las métricas asociadas con esas rutas.

TCP (*Protocolo de Control de Transmisión*): Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP (*Protocolo de Control de Transmisión /Protocolo Internet*): Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años ’70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Topología: Disposición física de los nodos y medios de red en una estructura de networking a nivel empresarial.

W

WAN (*Red de área amplia*) **:** Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por carriers comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN. Comparar con LAN y MAN.

Wi-fi (*Wíreless-Fidelity*): Esta denominación, aplicada al protocolo inalámbrico IEEE 802.11b significa que vía radio, mantiene con fidelidad las características de un enlace Ethernet cableado.